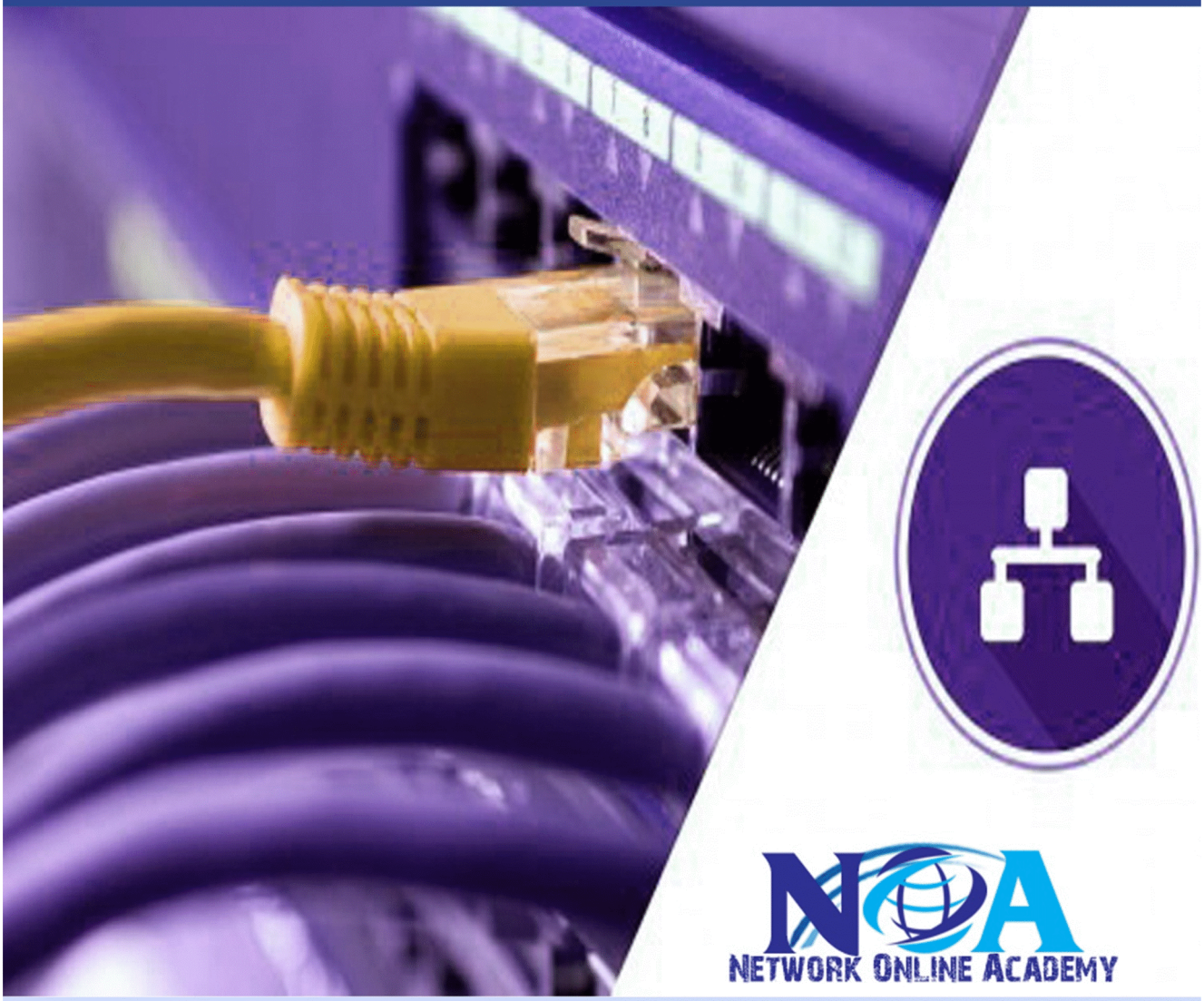
Implementing Cisco IP Switch Networks (300-115)

CCNP SWITCH Lab workbook version 2.1

Sikandar Shaik
CCIEx2(RS/SP)



NETWORK ONLINE ACADEMY

www.noasolutions.com

Sikandar Gouse Moinuddin

CCIE x2 (RS/SP)

About

Senior Technical Instructor/Network Consultant

Sikandar Shaik, a dual CCIE (RS/SP# 35012), is a highly experienced and extremely driven senior technical instructor and network consultant. He has been training networking courses for more than 10 years, teaching on a wide range of topics including Routing and Switching, Service Provider and Security (CCNA to CCIE). In addition, he has been developing and updating the content for these courses. He has assisted many engineers in passing out the lab examinations and securing certifications.

Sikandar Shaik is highly skilled at designing, planning, coordinating, maintaining, troubleshooting and implementing changes to various aspects of multi-scaled, multi-platform, multi-protocol complex networks as well as course development and instruction for a technical workforce in a varied networking environment. His experience includes responsibilities ranging from operating and maintaining PC's and peripherals to network control programs for multi-faceted data communication networks in LAN, MAN and WAN environments.

Sikandar Shaik has delivered instructor led trainings in several states in India as well as in abroad in countries like China, Kenya and UAE. He has also worked as a Freelance Cisco Certified Instructor globally for Corporate Major Clients.

41,052	11	207
Students	Courses	Reviews

Implementing Cisco IP Switched Networks (300-115)

- Implementing Cisco IP Switched Networks (SWITCH 300-115) is a 120-minute qualifying exam with 45–55 questions for the Cisco CCNP and CCDP certifications.
- The SWITCH 300-115 exam certifies the switching knowledge and skills of successful candidates.
- They are certified in planning,configuring, and verifying the implementation of complex enterprise switching solutions that use the Cisco Enterprise Campus Architecture.
- The SWITCH exam also covers highly secure integration of VLANs and WLANs.
- The following topics are general guidelines for the content that is likely to be included on the exam.
- However, other related topics may also appear on any specific version of the exam.
- To better reflect the contents of the exam and for clarity, the following guidelines may change at any time without notice.

INDEX

Auto-negotiation, Speed, and Duplex

By default, each Cisco switch port uses Ethernet auto-negotiation to determine the speed and duplex setting (half or full). The switches can also set their duplex setting with the duplex and their speed with the speed interface subcommand.

```
Switch(config)#int fa0/1
Switch(config-if)#speed ?
        10    Force 10 Mbps operation
        100   Force 100 Mbps operation
        auto  Enable AUTO speed configuration

Switch(config-if)#duplex ?
        auto  Enable AUTO duplex configuration
        full  Force full duplex operation
        half  Force half-duplex operation

Switch#sh interfaces fa0/1
      FastEthernet0/1 is down, line protocol is down (disabled)
        Hardware is Lance, address is 0030.f207.aa01 (bia 0030.f207.aa01)
        MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
          reliability 255/255, txload 1/255, rxload 1/255
        Encapsulation ARPA, loopback not set
        Keepalive set (10 sec)
        Half-duplex, 100Mb/s
```

To assign IP to a Switch

```
switch(config)# Interface Vlan 1
switch(config-if)# ip address <ip> <mask>
switch(config-if)# no shutdown
```

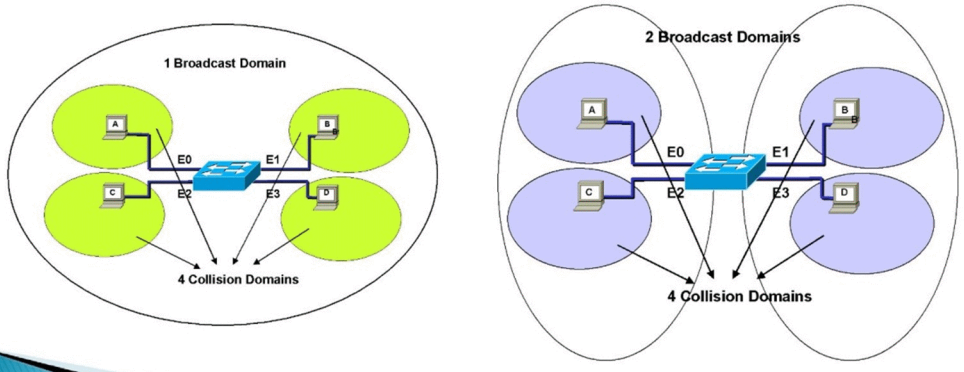
To assign Default Gateway to a Switch

```
Switch (config) #ip default-gateway 192.168.1.100
```

VLAN & Trunks

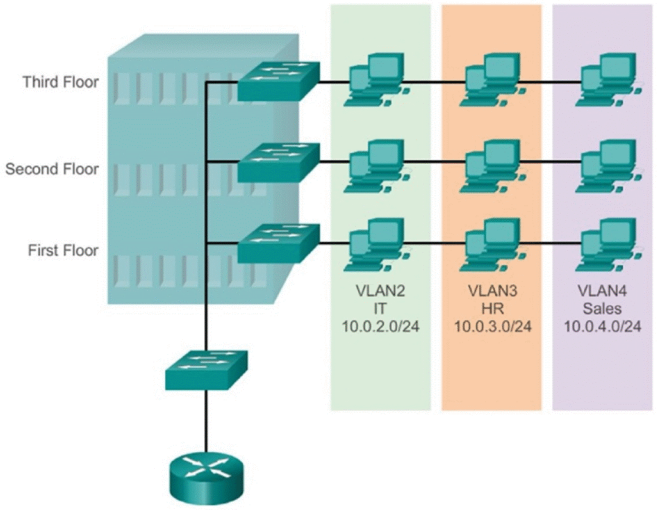
Virtual LAN

- Divides a Single Broadcast domain into Multiple Broadcast domains.
- A Layer 2 Security
- Vlan 1 is the default VLAN.
- We can create vlans from 2 – 1001
- Can be Configured on a Manageable switches only



Benefits of VLANs

- Limit the number of broadcast
- Better performance
- Security



Types of VLAN

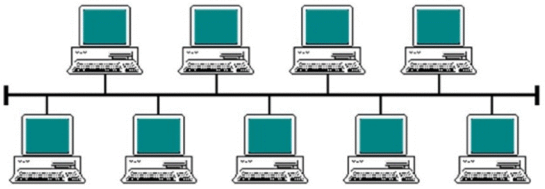
1. Static VLAN
2. Dynamic VLAN

VLAN Ranges

VLAN Range	Use
0, 4095	Reserved for system use only
1	Cisco default
2–1001	For Ethernet VLANs
1002–1005	Cisco defaults for FDDI and Token Ring
1006–4094	Ethernet VLANs only, unusable on specific legacy platforms

Static VLAN

- Static VLAN's are based on port numbers
- Need to manually assign a port on a switch to a VLAN
- Also called Port-Based VLANs
- One port can be a member of only one VLAN



Vlan Creation :

Switch(config)# **vlan <no>**
Switch(config-Vlan)# **name <name>**
Switch(config-Vlan)# **Exit**

Assigning ports in Vlan

Switch(config)# **interface <interface type> <interface no.>**
Switch(config-if)# **switchport mode access**
Switch(config-if)# **switchport access Vlan <no>**

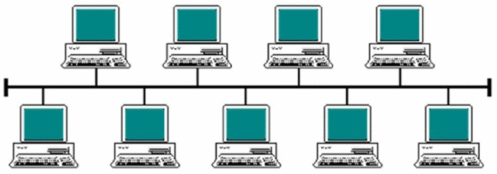
VLAN 1

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1,  Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

TASK: Create four VLANs (VLAN 10,20,30,40)

```
Switch(config)#vlan 10
Switch(config-vlan)#name sales

Switch(config-vlan)#vlan 20
Switch(config-vlan)#name
marketing

Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40

Switch(config-vlan)#end
```



Switch#sh vlan

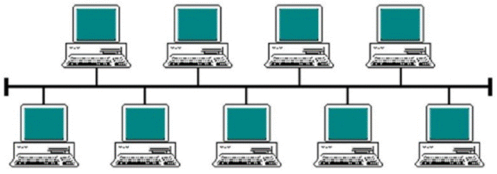
VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
10	sales	active	
20	marketing	active	
30	VLAN0030	active	
40	VLAN0040	active	

TASK :

Configure port fa0/8 in to vlan 10

Configure multiple ports (4 – 7 and 10) to vlan 20

```
Switch(config)#int f0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```



```
Switch(config)#interface range f0/4 - 7 , f0/10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

Switch#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/9, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24
10	sales	active	Fa0/8
20	marketing	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/10

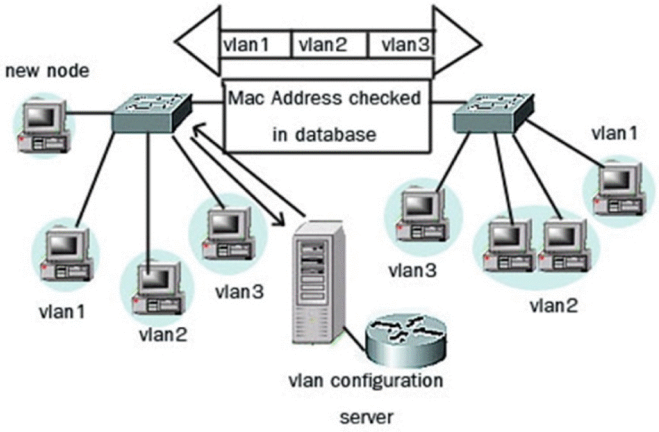
Dynamic VLAN

- Dynamic VLAN's are based on the MAC address of a PC
- Switch automatically assigns the port to a VLAN
- Each port can be a member of multiple VLAN's
- For Dynamic VLAN configuration, a software called VMPS(VLAN Membership Policy Server) is needed

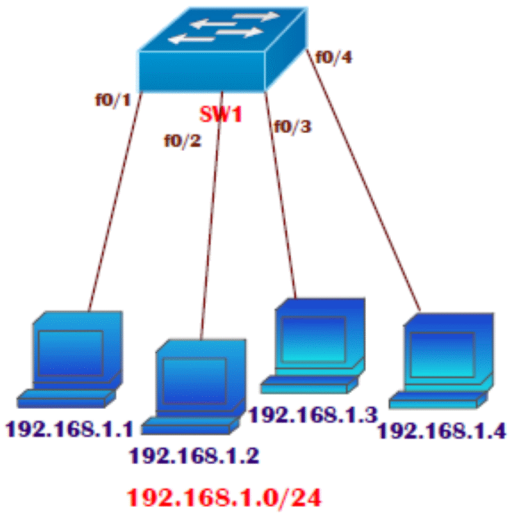
A VMPS Server Essentially Maps VLANS to MAC's

Entry	VLAN Membership	MAC Address
1	2	5D:FF:68:DE:22:0A
2	4	5A:09:DF:FF:41:12
3	4	1A:B4:4F:CC:35:32
4	12	8E:E3:FA:C8:B2:63
5	4	F2:3D:A9:00:37:42
6	4	C4:72:36:FF:A2:61
7	12	5B:90:03:BB:BC:25
8	12	B9:42:27:A3:7F:1F
9	2	DD:0D:26:52:78:35
10	2	C4:42:25:1F:DA:94

The VMPS server contains a database with all VLAN to MAC address mapping, allowing the "dynamic" VLAN configuration of these hosts, no matter where they are located within the network.



LAB –Verify VLAN



STEPS:

1. Ping between 192.168.1.1 and 192.168.1.3
   a. (they can communicate with each other and they are on the same network (logically) and same VLAN (default vlan 1)
2. Create VLAN 20
3. Shift port f0/3 , f0/4 in to VLAN 20
4. Ping between 192.168.1.1 and 192.168.1.3
   a. they cannot communicate with each other and they are on the same network (logically) but on different VLAN (VLAN1 and vlan 20)

Switch#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

PC>ipconfig

IP Address.....: 192.168.1.1

Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=19ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=12ms TTL=128
Reply from 192.168.1.3: bytes=32 time=9ms TTL=128
Reply from 192.168.1.3: bytes=32 time=7ms TTL=128
Reply from 192.168.1.3: bytes=32 time=8ms TTL=128

PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=10ms TTL=128
Reply from 192.168.1.4: bytes=32 time=8ms TTL=128
Reply from 192.168.1.4: bytes=32 time=8ms TTL=128
Reply from 192.168.1.4: bytes=32 time=9ms TTL=128

All the Four devices in the LAN can communicate with each other and they are on the same network (logically) and same VLAN (default vlan 1)

TASK: Create Vlan 20 And Shift The Ports 3 And 4 In To Vlan 20

```
Switch(config)#vlan 20
Switch(config-vlan)#name  SALES
Switch(config-vlan)#exit

Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20

Switch#sh vlan
```

VLAN Name Status Ports

```
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig1/1, Gig1/2
20   SALES                            active    Fa0/3, Fa0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

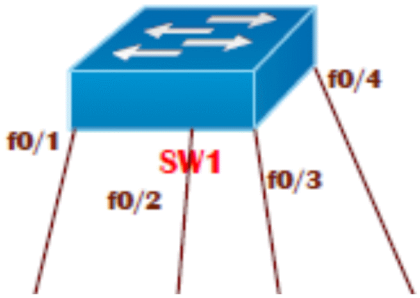
```
PC>ipconfig

   IP Address.....: 192.168.1.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.1.100
```

```
PC>ping 192.168.1.2

   Pinging 192.168.1.2 with 32 bytes of data:
   Reply from 192.168.1.2: bytes=32 time=11ms TTL=128
   Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
   Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
   Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
```

```
PC>ping 192.168.1.3

   Pinging 192.168.1.3 with 32 bytes of data:
   Request timed out.
   Request timed out.
   Request timed out.
   Request timed out.
```

```
PC>ping 192.168.1.4

   Pinging 192.168.1.4 with 32 bytes of data:
   Request timed out.
   Request timed out.
   Request timed out.
   Request timed out.
```

LAB -2 CREATING BASIC VLAN CONFIGURATION ON SWITCHES



TASK:

- Create four VLANs (VLAN 10,20,30,40)
- Configure port fa0/8 in to vlan 10
- Configure multiple ports (4 – 7 and 10) to vlan 20

```
Switch(config)#vlan 10
Switch(config-vlan)#name sales

Switch(config-vlan)#vlan 20
Switch(config-vlan)#name marketing

Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#end

Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
10   sales                             active
20   marketing                         active
30   VLAN0030                          active
40   VLAN0040                          active
```

There are no active ports in the new vlan which we created

To shift the ports

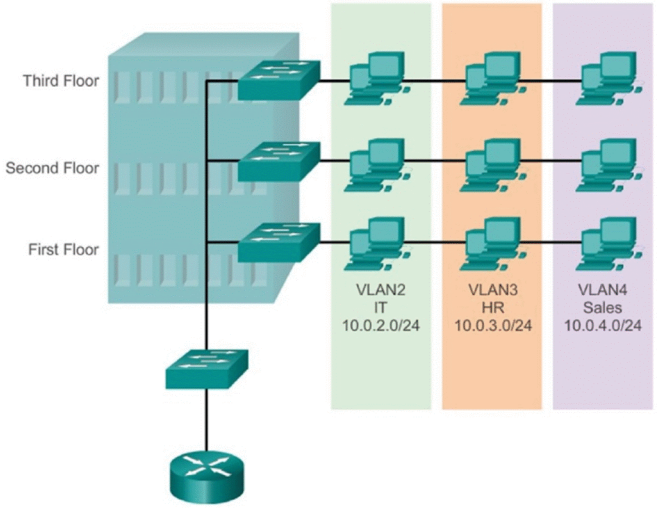
```
Switch(config)#int f0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit

Switch(config)#interface range f0/4 - 7 , f0/10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

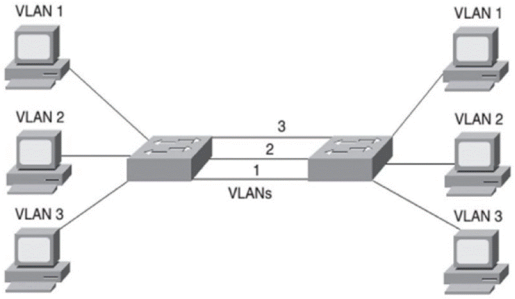
Switch#sh vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3,
                                                 Fa0/9, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
10   sales                             active    Fa0/8
20   marketing                         active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/10
```

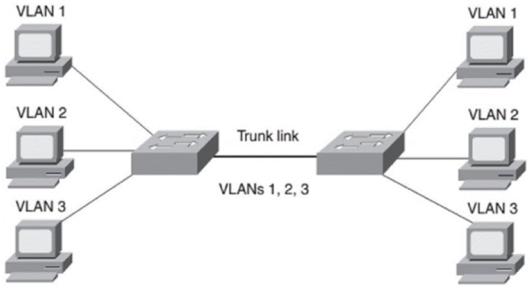
Trunking

- A single VLAN can span over Multiple Switches





Passing VLAN Traffic Using Separate Links for each VLAN



Passing VLAN Traffic Using Single Links

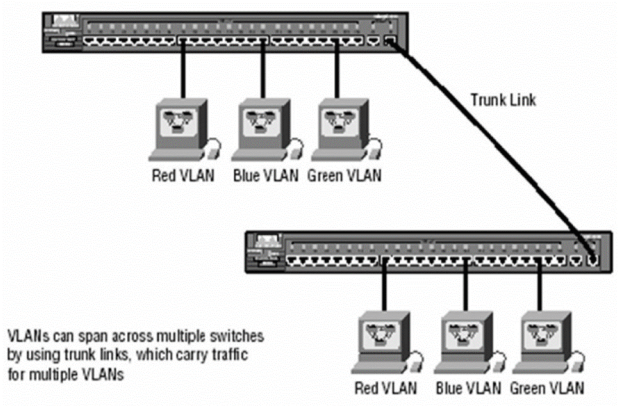
Types of links/ports

Access links

- Connecting to end devices (Hosts or router)
- part of one VLAN

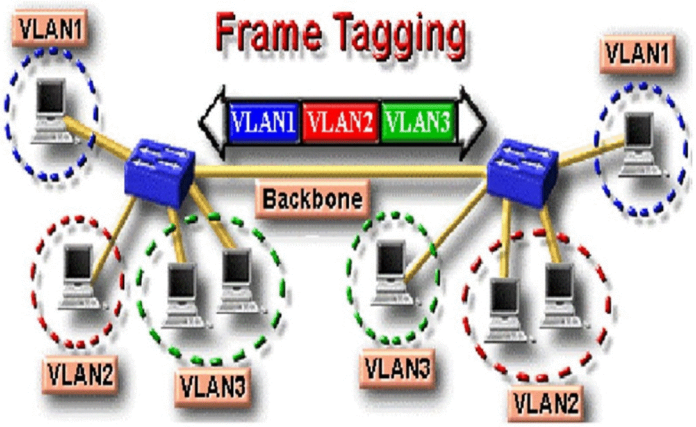
Trunk links

- Do not belong to any VLAN
- carry multiple VLANs traffic.
- link between two switches.



Frame Tagging

- In oder to make sure that same vlan users on different switches communicate with each other there is a method of tagging happens on trunk links .
- Tag is added before a frame is send and removed once it is received on trunk link.
- Frame tagging happens only on the trunk links



Trunking protocols

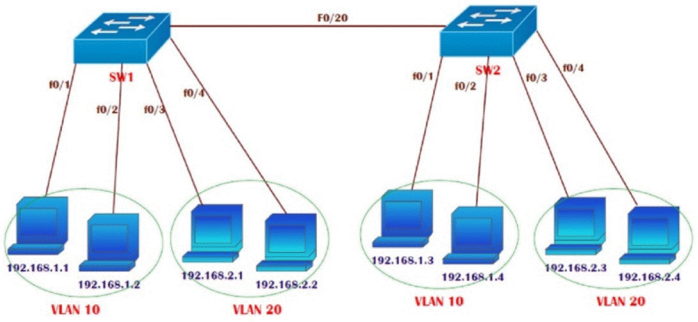
ISL	IEEE 802.1Q
• It's a Cisco proprietary	• Open standard
• It works with Ethernet, Token ring, FDDI	• It works only on Ethernet
• It adds 30 bytes of tag	• Only 4 Byte tag will be added to original frame.
• All VLAN traffic is tagged	

Trunking Configuration

Switch(config)# **interface <interface type> <interface no.>**
Switch(config-if)# **switchport mode trunk**
Switch(config-if)# **switchport trunk encapsulation dot1q/ISL**

SW-2#sh interfaces trunk

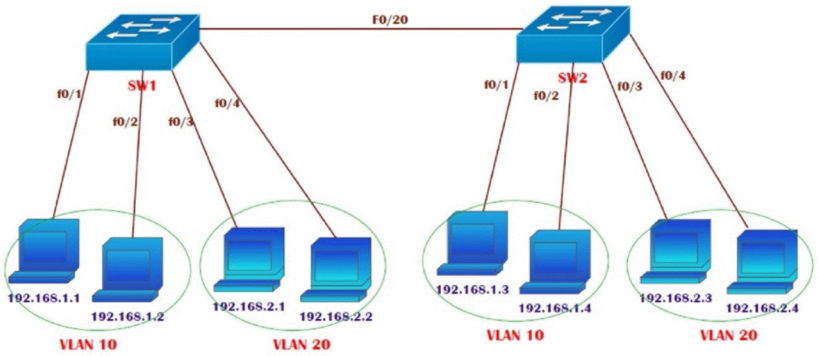
Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1



LAB : Trunking

TASK:

1. Create Vlan 10 , Vlan 20 on both Switches
2. Shift ports in to their respective VLAN as per the diagram.
3. Confiure F0/20 port between SW1 and SW2 as Trunk link
4. Ensure That users of same VLAN on different Switches must communicate with each other



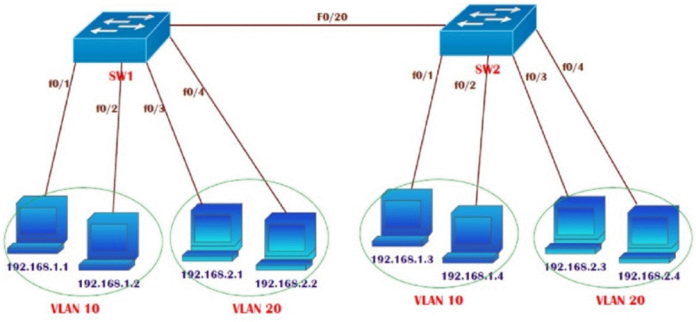
Allowed Vlan list on trunk Link

- By default, a switch transports all active VLANs (1 to 4094) over a trunk link.
- An active VLAN is one that has been defined on the switch and has ports assigned to carry it.
- There might be times when the trunk link should not carry all VLANs.

SW-2#sh interfaces trunk

Port	*Mode*	*Encapsulation*	*Status*	*Native vlan*
Fa0/20	*on*	*802.1q*	*trunking*	*1*

Port	*Vlans allowed on trunk*
Fa0/20	*1-1005*



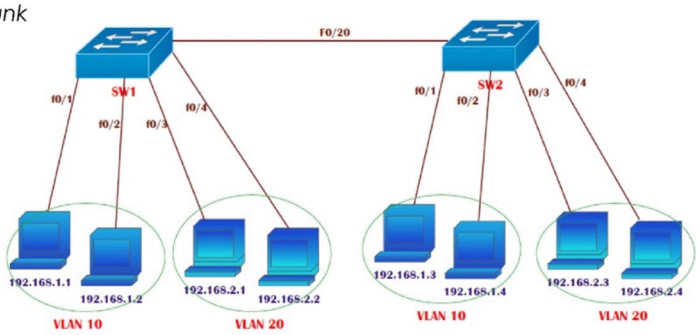
Allowed Vlan list on trunk Link(contd)

*SW-x(config-if)#**switchport trunk allowed vlan 10,20,30,40***

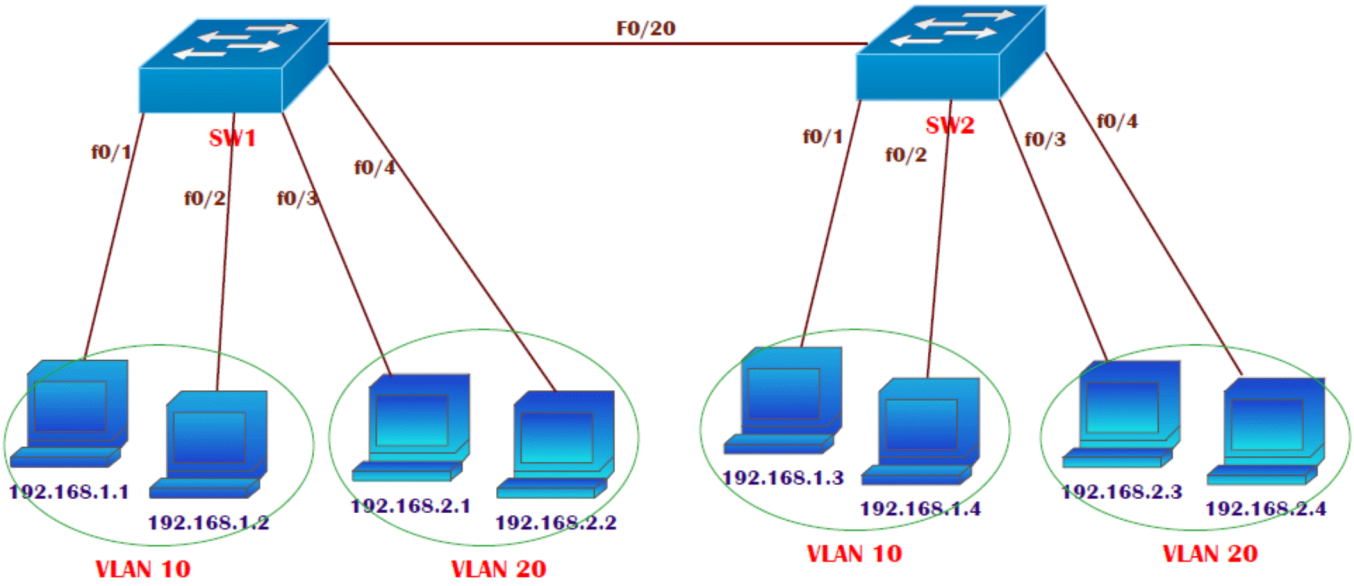
SW-1#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/20	10,20,30,40



LAB: TRUNKING



TASK:

- Create Vlan 10 , Vlan 20 on both Switches
- Shift ports in to their respective VLAN as per the diagram.
- Confiure F0/20 port between SW1 and SW2 as Trunk link
- Ensure That users of same VLAN on different Switches must communicate with each other

On SW-1

```
Switch(config)#hostname SW-1
SW-1(config)#interface range f0/1 - 2
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
SW-1(config-if-range)#exit

SW-1(config)#interface range f0/3 - 4
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 20
SW-1(config-if-range)#end

SW-1#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
```

```
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gig1/1, Gig1/2
10   VLAN0010                       active    Fa0/1, Fa0/2
20   VLAN0020                       active    Fa0/3, Fa0/4
1002 fddi-default                   act/unsup
1003 token-ring-default             act/unsup
1004 fddinet-default                act/unsup
1005 trnet-default                  act/unsup
```

On SW-2

```
Switch(config)#hostname SW-2
SW-2(config)#interface range f0/1 - 2
SW-2(config-if-range)#switchport mode access
SW-2(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
SW-2(config-if-range)#exit

SW-2(config)#interface range f0/3 - 4
SW-2(config-if-range)#switchport mode access
SW-2(config-if-range)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SW-2(config-if-range)#end

SW-2#sh vlan
VLAN Name                           Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                        active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12

                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gig1/1, Gig1/2
10   VLAN0010                       active    Fa0/1, Fa0/2
20   VLAN0020                       active    Fa0/3, Fa0/4
1002 fddi-default                   act/unsup
1003 token-ring-default             act/unsup
1004 fddinet-default                act/unsup
1005 trnet-default                  act/unsup
```

From PC 192.168.1.1

PC>ipconfig

IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=13ms TTL=128
Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128

PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

From PC 192.168.2.1

PC>ipconfig

IP Address.....: 192.168.2.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.100

PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=17ms TTL=128
Reply from 192.168.2.2: bytes=32 time=7ms TTL=128
Reply from 192.168.2.2: bytes=32 time=9ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128

SERVER>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Request timed out.
Request timed out.

Request timed out.
Request timed out.

SERVER>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

NOTE:

- From the above verification
- Users of the same VLAN connected on the same switch can ping each other
- Same vlan users on different switches are not able to ping each other
- In oder to communicate between same vlan on different switches , there should be trunking configured on link (f0/20) between the switches

To configure trunking

SW-1(config)#interface fastEthernet 0/20

SW-1(config-if)#switchport mode trunk

SW-1(config-if)#switchport trunk encapsulation dot1q

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed state to up

SW-2(config)#int f0/20

SW-2(config-if)#switchport mode trunk

SW-2(config-if)#switchport trunk encapsulation dot1q

SW-1#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1

Port Vlans allowed on trunk
Fa0/20 1-1005
Port Vlans allowed and active in management domain
Fa0/20 1,10,20
Port Vlans in spanning tree forwarding state and not pruned
Fa0/20 1,10,20

SW-2#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1

Port Vlans allowed on trunk
Fa0/20 1-1005

Port Vlans allowed and active in management domain
Fa0/20 1,10,20
Port Vlans in spanning tree forwarding state and not pruned
Fa0/20 1,10,20

From PC 192.168.1.1

PC>ipconfig

IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=17ms TTL=128
Reply from 192.168.1.3: bytes=32 time=13ms TTL=128
Reply from 192.168.1.3: bytes=32 time=12ms TTL=128
Reply from 192.168.1.3: bytes=32 time=10ms TTL=128

PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=25ms TTL=128
Reply from 192.168.1.4: bytes=32 time=14ms TTL=128
Reply from 192.168.1.4: bytes=32 time=12ms TTL=128
Reply from 192.168.1.4: bytes=32 time=13ms TTL=128

From PC 192.168.2.1

PC>ipconfig

IP Address.....: 192.168.2.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.100

PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=13ms TTL=128
Reply from 192.168.2.3: bytes=32 time=12ms TTL=128
Reply from 192.168.2.3: bytes=32 time=13ms TTL=128
Reply from 192.168.2.3: bytes=32 time=13ms TTL=128

PC>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

```
Reply from 192.168.2.4: bytes=32 time=26ms TTL=128
Reply from 192.168.2.4: bytes=32 time=12ms TTL=128
Reply from 192.168.2.4: bytes=32 time=12ms TTL=128
Reply from 192.168.2.4: bytes=32 time=13ms TTL=128
```

TASK:

- Configure The Trunk Link Such That It Only Allow The Vlan 10 , 20, 30 , 40 Traffic Should Only Be Allowed (No Other Vlan Traffic Should Be Send)

On both switches (SW1/SW2)

```
SW-x(config)#int f0/20
SW-x(config-if)#switchport trunk allowed vlan ?

  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  none    no VLANs
  remove  remove VLANs from the current list

SW-x(config-if)#switchport trunk allowed vlan 10,20,30,40

SW-1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/20      10,20,30,40
Port        Vlans allowed and active in management domain
Fa0/20      10,20
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20

SW-2#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/20      10,20,30,40

Port        Vlans allowed and active in management domain
Fa0/20      10,20
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20
```

TASK:

- Create vlan 50, 60,70,80 on both switches
- Configure the trunk link f0/20 to add vlan 50 ,60,70,80 to the existing trunk allowed list

On both switches (SW1/SW2)

```
SW-x(config)#vlan 50
SW-x(config-vlan)#vlan 60
SW-x(config-vlan)#vlan 70
SW-x(config-vlan)#vlan 80
SW-x(config-vlan)#end

SW-x(config-if)#switchport trunk allowed vlan add 50,60,70,80

SW-1#sh interfaces trunk
Port        Mode         Encapsulation Status        Native vlan
Fa0/20      on           802.1q        trunking      1
Port        Vlans allowed on trunk
Fa0/20      10, 20,30,40,50,60,70,80
Port        Vlans allowed and active in management domain
Fa0/20      10,20,50,60
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20,50,60

SW-2#sh interfaces trunk
Port        Mode         Encapsulation  Status       Native vlan
Fa0/20      on           802.1q         trunking     1
Port        Vlans allowed on trunk
Fa0/20      10,20,30,40,50,60,70,80
Port        Vlans allowed and active in management domain
Fa0/20      10,20,50,60
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20,50,60
```

TASK

- Configure the trunk link f0/20 to remove vlan 70,80 to the existing trunk allowed list

```
SW-1(config)#int f0/20
SW-1(config-if)#switchport trunk allowed vlan remove 70,80

SW-1#sh interfaces trunk
Port        Mode         Encapsulation Status        Native vlan
Fa0/20      on           802.1q        trunking      1
Port        Vlans allowed on trunk
Fa0/20      10,20,30,40,50,60
Port        Vlans allowed and active in management domain
```

Fa0/20 10,20,50,60
Port Vlans in spanning tree forwarding state and not pruned
Fa0/20 10,20,50,60

SW-2#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1

Port Vlans allowed on trunk
Fa0/20 10,20,30,40,50,60
Port Vlans allowed and active in management domain
Fa0/20 10,20,50,60
Port Vlans in spanning tree forwarding state and not pruned
Fa0/20 10,20,50,60

DTP (DYNAMIC TRUNKING PROTOCOL)

Trunking can be done dynamically through negotiation process

```
Switch# sh dtp
        Global DTP information
          Sending DTP Hello packets every 30 seconds
          Dynamic Trunk timeout is 300 seconds
          0 interfaces using DTP
```

DTP MODES

DESIRABLE:

- desires to become trunk (always want to become trunk)
- Sends and reply to DTP messages
- It becomes a trunk if the port on the other switch is set to **trunk, dynamic desirable** or **dynamic auto** mode.

AUTO:

- Only reply to DTP messages (not send)
- Default mode on most of the modern switches
- It becomes a trunk if the other end is set to **trunk** or **dynamic desirable** mode.

TRUNK

- Configuring trunk manually
- The port still negotiates trunking with the port on the other end of the link.

ACCESS

- Configuring access manually
- The port is a user port in a single VLAN.

NO-NEGOTIATE

- Turn off DTP messages (disable DTP).
- The port is a trunk and does not do DTP negotiation with the other side of the link.

Switchport Mode Interactions

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

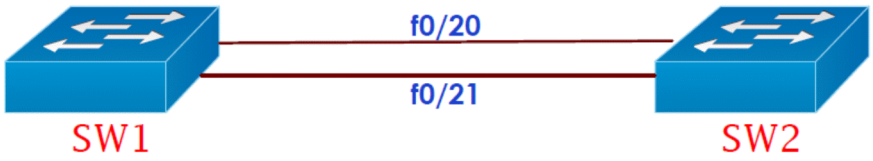
Note: Table assumes DTP is enabled at both ends.

- show dtp interface – **to determine current setting**

DTP can be disabled either by

1. configuring as access port using **switchport mode access**
2. or using **switchport nonegotiate** commands

LAB: VERIFYING DTP



TASK:

- Configure f0/20 of SW1 to actively negotiate the DTP messages and SW2 f0/20 port should only reply to the DTP messges
- Configure f0/21 of SW1 and SW2 should not negotiate any DTP essages

Sw-1# sh interfaces fa0/20 switchport
Name: Fa0/20
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native

On SW-1

Sw-1(config)#int f0/20
Sw-1(config-if)#switchport mode ?
access Set trunking mode to ACCESS unconditionally
dynamic Set trunking mode to dynamically negotiate access or trunk mode
trunk Set trunking mode to TRUNK unconditionally

Sw-1(config-if)#switchport mode dynamic desirable

SW-1#sh interfaces fa0/20 switchport
Name: Fa0/20
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q

SW-1# sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	auto	n-802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/20	1-1005

Switch#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	auto	n-802.1q	trunking	1

```
Port        Vlans allowed on trunk
Fa0/20      1-1005
Port        Vlans allowed and active in management domain
Fa0/20      1
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      1
```

TASK: Configure SW1 and SW2 to Configure Manaul Trunk and Disable the DTP negotiation Process.

On SW1/SW2

```
Sw-x(config)#int f0/21
Sw-x(config-if)#switchport mode trunk
Sw-x(config-if)#switchport trunk encapsulation dot1q
Sw-x(config-if)#switchport nonegotiate
```

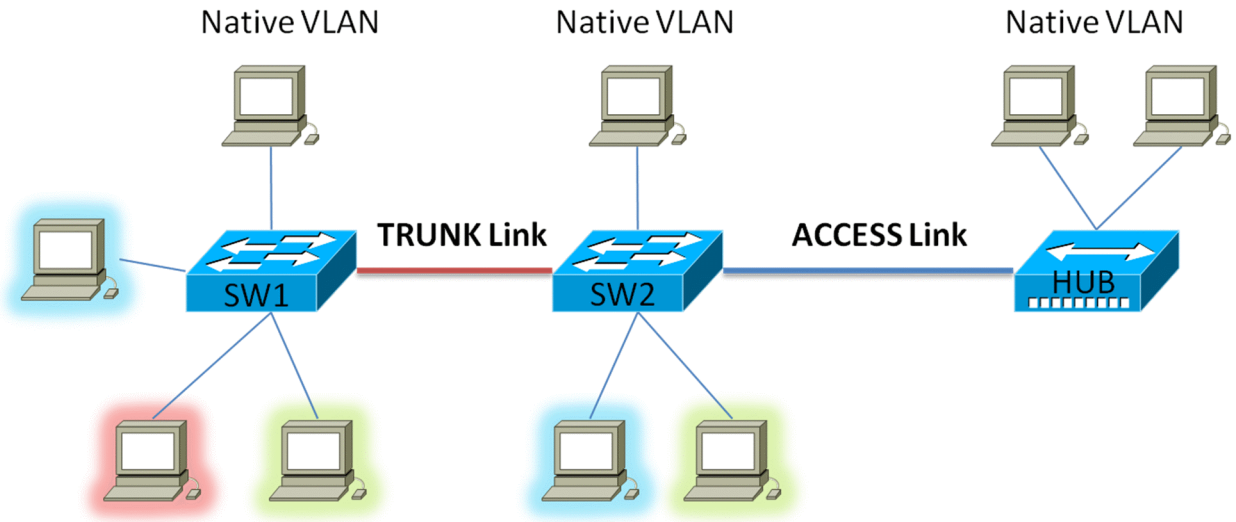
Sw-1#sh interfaces trunk

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      auto         n-802.1q       trunking      1
Fa0/21      on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/20      1-1005
Fa0/21      1-1005
Port        Vlans allowed and active in management domain
Fa0/20      1
Fa0/21      1
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      1
Fa0/21      1
```

Sw-2#sh interfaces trunk

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      auto         n-802.1q       trunking      1
Fa0/21      on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/20      1-1005
Fa0/21      1-1005
Port        Vlans allowed and active in management domain
Fa0/20      1
Fa0/21      1
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      1
Fa0/21      none
```

NATIVE VLAN

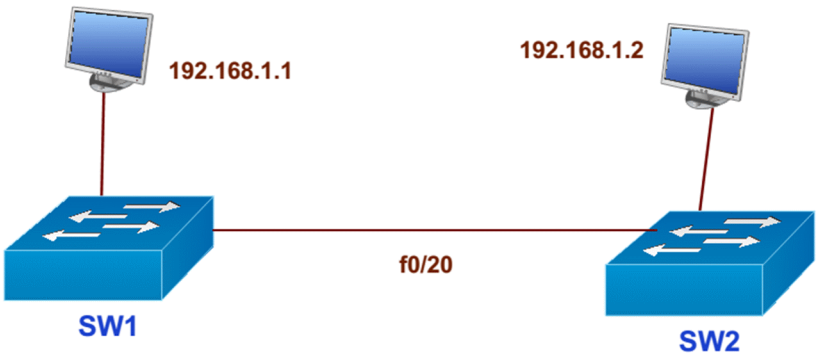


- If a packet is received on a dot1q link, that does not have VLAN tagged, it is assumed that it belongs to native VLAN.
- Untagged frames must place into a VLAN by the receiving switch, the native VLAN is the VLAN used.
- When a switch receives an untagged frame on a tagged interface it is assumed membership of the Native VLAN.
- For Cisco switches the Native VLAN ID must match on both end of the trunk.
- By default the Native VLAN is 1.
- Best Practice is to configure the Native VLAN ID to VLAN 666 and to ensure that this VLAN is not used anywhere in the network.
- Use this new vlan as the native vlan. No ports should be assigned to the native vlan ie. you do not have any end devices in the native vlanThe number "666" helps people to remember this.
- An attacker who attempts to use the VLAN hopping attack will end up in a dead VLAN that has no hosts to leverage.

This message appears when the native VLAN is mismatched on the two Cisco switches:

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEhernet1/1 (2), with D-R3550-9B GigabitEthernet0/1 (1)

LAB: Native VLAN



TASK:

- Connect Devices and assign the IP addressing as per the diagram.
- Create vlan 999 on both switches.
- Configure f0/20 port as trunk link
- Ensure that vlan 999 should be native vlan on both trunks.
- Verify the connectivity between PC (192.168.1.1 and 192.168.1.2).

PC>ipconfig

FastEthernet0 Connection:(default port)
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 0.0.0.0

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=12ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128

On SW1/SW2

SWx(config)#vlan 999
SWx(config-vlan)#end

SWx(config)#int f0/20
SWx(config-if)#switchport trunk encapsulation dot1q
SWx(config-if)#switchport mode trunk

SW2#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1

Port Vlans allowed on trunk

```
Fa0/20      1-1005
Port        Vlans allowed and active in management domain
Fa0/20      1
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      1
```

```
PC>ping 192.168.1.2
    Pinging 192.168.1.2 with 32 bytes of data:
    Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
    Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
    Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
    Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
```

TASK: change native vlan to 999 on SW1 and verify connectivity

```
SW1(config)#int f0/20
SW1(config-if)#switchport trunk native vlan 999
SW1(config-if)#end
```

```
SW1#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/20 (999), with SW2 FastEthernet0/20 (1).
```

```
PC>ping 192.168.1.2
    Pinging 192.168.1.2 with 32 bytes of data:
    Request timed out.
    Request timed out.
    Request timed out.
    Request timed out.
```

```
SW1#sh interfaces trunk
        Port        Mode         Encapsulation  Status        Native vlan
        Fa0/20      on           802.1q         trunking      999
        Port        Vlans allowed on trunk
        Fa0/20      1-1005
        Port        Vlans allowed and active in management domain
        Fa0/20      1
        Port        Vlans in spanning tree forwarding state and not pruned
        Fa0/20      1
```

```
SW1#sh interfaces f0/20 switchport
        Name: Fa0/20
        Switchport: Enabled
        Administrative Mode: dynamic auto
```

Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 999 (VLAN0999)
Voice VLAN: none

SW2#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/20	1-1005

Port	Vlans allowed and active in management domain
Fa0/20	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/20	1

SW2(config)#int f0/20
SW2(config-if)#switchport trunk native vlan 999
SW2(config-if)#end

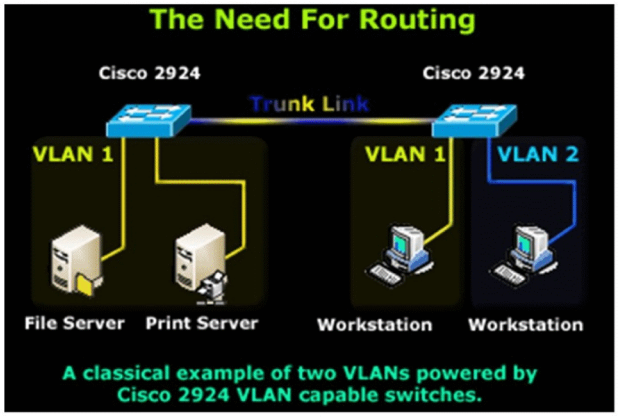
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128

Troubleshooting Vlan and Trunks

- Same netwok
- Same vlan
- Trunking (mode)
- Allowed vlan on the trunk link
- Native lan must match

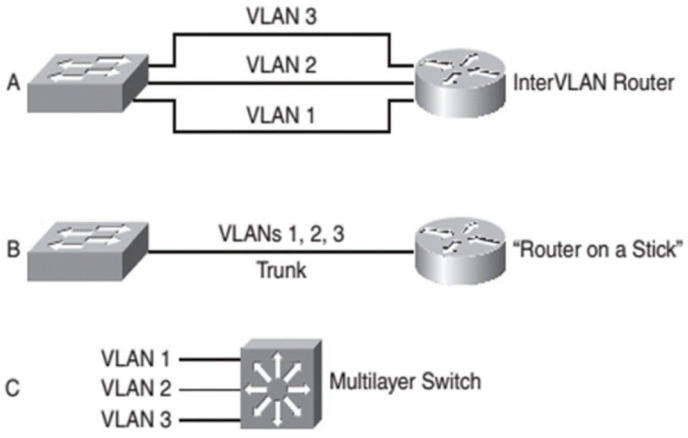
Inter Vlan Routing



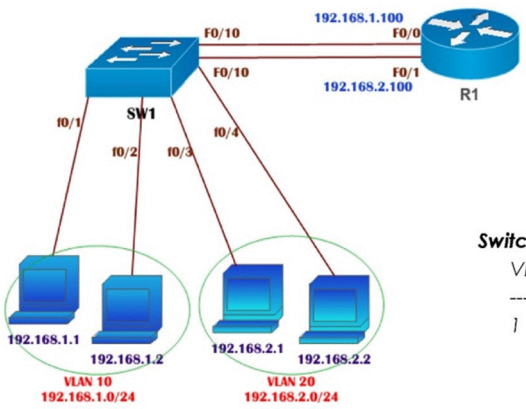
- packets in one VLAN cannot cross into another VLAN.
- To transport packets between VLANs, you must use a Layer 3 device.
- The router must have a physical or logical connection to each VLAN so that it can forward packets between them.
- This is known as inter-VLAN routing.
- Inter-VLAN routing can be performed by an external router that connects to each of the VLANs on a switch.

Inter-Vlan Routing Methods

A. Separate Physical Gateway on Router
B. Using Sub-interfaces
C. Using Layer 3 Switch



Inter-Vlan Routing using Separate Physical Gateway on Router

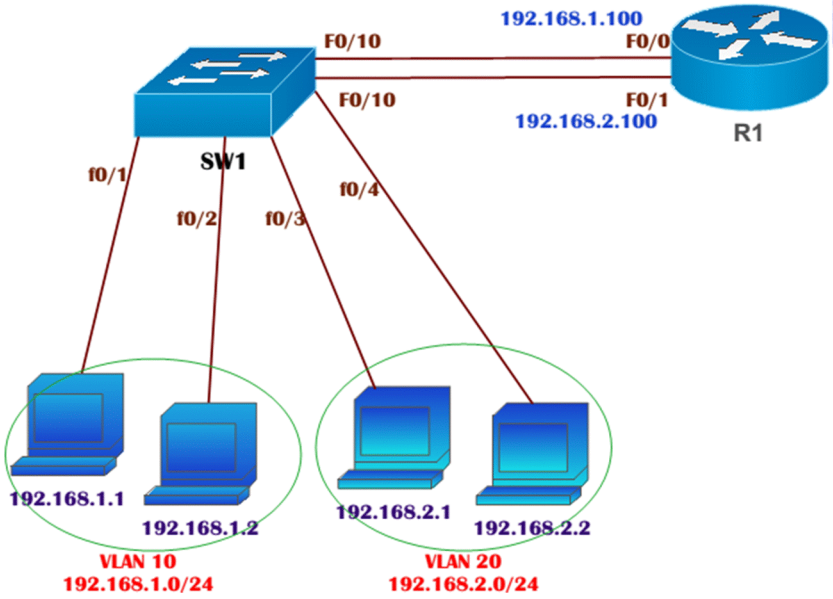



```
Router(config)#interface FastEthernet0/0
Router(config-if)# ip address 192.168.1.100 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface FastEthernet0/1
Router(config-if)# ip address 192.168.2.100 255.255.255.0
Router(config-if)#no shutdown
```

```
Switch#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   sales                             active    Fa0/1, Fa0/2, Fa0/10
20   marketing                         active    Fa0/3, Fa0/4, Fa0/11
1002 fddi-default                      act/unsup
```

TASK

- Create Vlan 10, Vlan 20 on SW1 and assign ports in to their respective VLAN as per the diagram.
- Ensure That users of VLAN 10 and 20 communicate with each other




```
Switch(config)#vlan 10
Switch(config-vlan)#name sales
```

```
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name marketing
Switch(config-vlan)#exit

Switch(config)#interface FastEthernet0/1
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access

Switch(config-if)#interface FastEthernet0/2
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access

Switch(config-if)#interface FastEthernet0/3
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode access

Switch(config-if)#interface FastEthernet0/4
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode access
Switch(config-if)#exit

Switch(config)#interface FastEthernet0/10
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access

Switch(config-if)#interface FastEthernet0/11
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode access
Switch(config-if)#end

Switch#sh vlan
 VLAN Name                              Status    Ports
 ---- --------------------------------- --------- -------------------------------
 1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                  Fa0/9, Fa0/12, Fa0/13, Fa0/14
                                                  Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                  Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                  Fa0/23, Fa0/24, Gig1/1, Gig1/2
 10   sales                             active    Fa0/1, Fa0/2, Fa0/10
 20   marketing                         active    Fa0/3, Fa0/4, Fa0/11
 1002 fddi-default                      act/unsup

Router(config)#interface FastEthernet0/0
```

```
Router(config-if)# ip address 192.168.1.100 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface FastEthernet0/1
Router(config-if)# ip address 192.168.2.100 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#end
```

```
Router#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.100   YES manual up                    up
FastEthernet0/1        192.168.2.100   YES manual up                    up
```

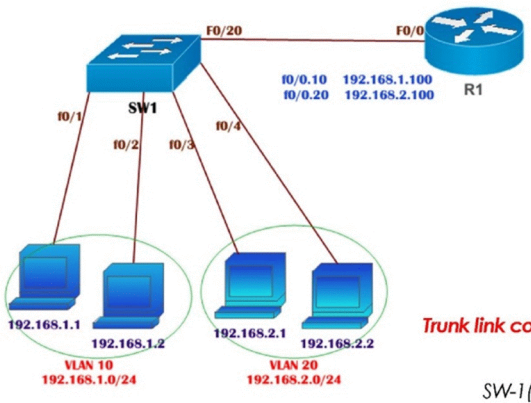
```
Router#sh ip route
Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
```

```
PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: ::
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.1: bytes=32 time=0ms TTL=127
Reply from 192.168.2.1: bytes=32 time=0ms TTL=127
Reply from 192.168.2.1: bytes=32 time=0ms TTL=127
```

```
PC>tracert 192.168.2.1
Tracing route to 192.168.2.1 over a maximum of 30 hops:
  1   13 ms     0 ms      0 ms      192.168.1.100
  2   0 ms      0 ms      0 ms      192.168.2.1
Trace complete.
```

INTER VLAN-ROUTING USING ROUTER (Router On Stick)



SW-1#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig1/1, Gig1/2
10	VLAN0010	active	Fa0/1, Fa0/2
20	VLAN0020	active	Fa0/3, Fa0/4

Trunk link configuration

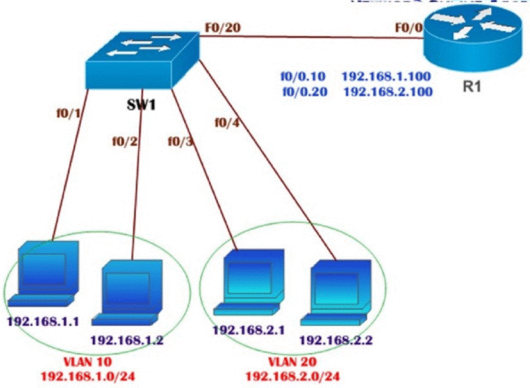
*SW-1(config)#**interface fastEthernet 0/20***

(interface facing Router)

*SW-1(config-if)#**switchport mode trunk***

*SW-1(config-if)#**switchport trunk encapsulation dot1q***

INTER VLAN-ROUTING USING ROUTER (Router On Stick)



Creating sub interfaces on router interface f0/0

*R-1(config)#**int fa0/0***
*R-1(config-if)# **no shutdown***
*R-1(config-if)# **exit***

*R-1(config)#**int fa0/0.10***
*R-1(config-sub-if)# **encapsulation dot1Q 10***

It should be the exact vlan no (vlan 10)

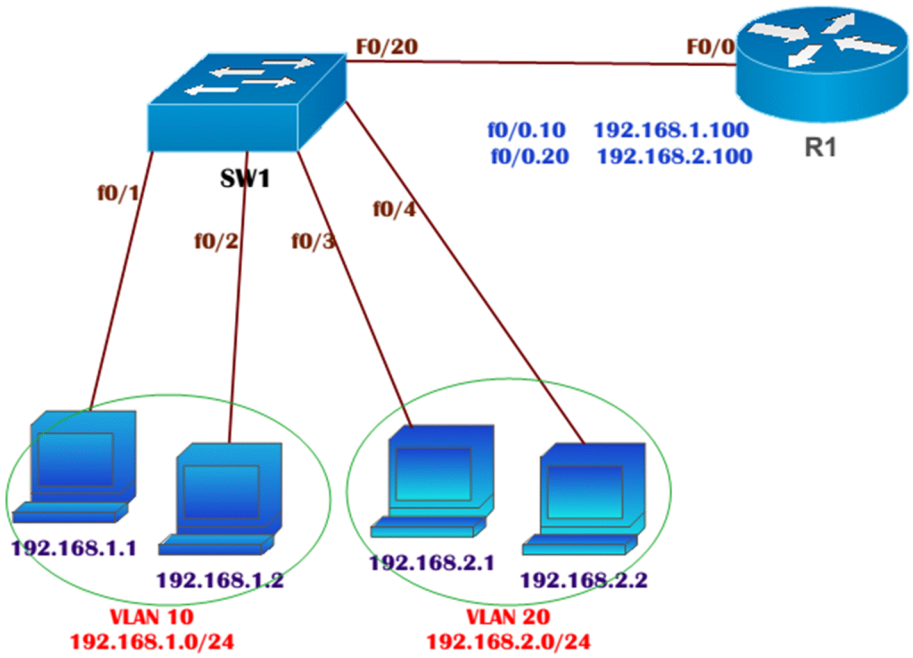
*R-1(config-sub-if)# **ip add 192.168.1.100 255.255.255.0***
*R-1(config-sub-if)# **exit***

*R-1(config)#**int fa0/0.20***
*R-1(config-sub-if)# **encapsulation dot1Q 20***

It should be the exact vlan no (vlan 20)

R-1(config-sub-if)# ip add 192.168.2.100 255.255.255.0

LAB INTER VLAN-ROUTING USING ROUTER (Router on Stick)



TASK:

- Create Vlan 10 , Vlan 20 on SW1
- Shift ports in to their respective VLAN as per the diagram.
- Confiure F0/20 port as Trunk link.
- Create sub interfaces on router port f0/0
- Ensure That users of VLAN 10 and 20 communicate with each other

On SW-1

```
Switch (config)#hostname SW-1
SW-1(config)#interface range f0/1 - 2
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 10

% Access VLAN does not exist. Creating vlan 10

SW-1(config-if-range)#exit

SW-1(config)#interface range f0/3 - 4
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 20
SW-1(config-if-range)#end
```

SW-1#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8
			Fa0/9, Fa0/10, Fa0/11, Fa0/12
			Fa0/13, Fa0/14, Fa0/15, Fa0/16
			Fa0/17, Fa0/18, Fa0/19, Fa0/20
			Fa0/21, Fa0/22, Fa0/23, Fa0/24
			Gig1/1, Gig1/2
10	VLAN0010	active	Fa0/1, Fa0/2
20	VLAN0020	active	Fa0/3, Fa0/4
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Trunk link configuration

SW-1(config)#interface fastEthernet 0/20

(Interface facing Router)

SW-1(config-if)#switchport mode trunk

SW-1(config-if)#switchport trunk encapsulation dot1q

- A router on a stick can be used to route between VLANs using either ISL or 802.1Q as the trunking protocol.
- A router on a stick requires subinterfaces, one for each VLAN.

Creating sub interfaces on router interface f0/0

R-1(config)#int fa0/0
R-1(config-if)# no shutdown
R-1(config-if)# exit

R-1(config)#int fa0/0.10
R-1(config-sub-if)# encapsulation dot1Q 10

It should be the exact vlan no (vlan 10)

R-1(config-sub-if)# ip add 192.168.1.100 255.255.255.0
R-1(config-sub-if)# exit

R-1(config)#int fa0/0.20
R-1(config-sub-if)# encapsulation dot1Q 20

It should be the exact vlan no (vlan 20)

R-1(config-sub-if)# ip add 192.168.2.100 255.255.255.0

Router#sh ip int brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	up	up
FastEthernet0/0.10	192.168.1.100	YES	manual	up	up
FastEthernet0/0.20	192.168.2.100	YES	manual	up	up

Verify connectivity

PC>ipconfig

IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>ping 192.168.2.1

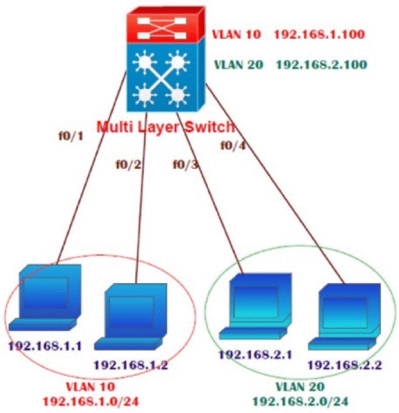
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.1: bytes=32 time=62ms TTL=127
Reply from 192.168.2.1: bytes=32 time=125ms TTL=127
Reply from 192.168.2.1: bytes=32 time=109ms TTL=127

PC>tracert 192.168.2.1

Tracing route to 192.168.2.1 over a maximum of 30 hops:

1	47 ms	63 ms	62 ms	192.168.1.100
2	109 ms	125 ms	78 ms	192.168.2.1

Inter Vlan-Routing Using MLS



SW-1#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig1/1, Gig1/2
10	VLAN0010	active	Fa0/1, Fa0/2
20	VLAN0020	active	Fa0/3, Fa0/4

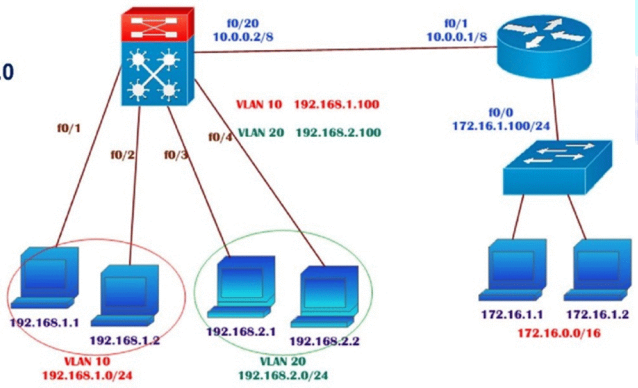
```
Switch(config)#int vlan 10
Switch(config-if)#ip address 192.168.1.100 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#int vlan 20
Switch(config-if)#ip address 192.168.2.100 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Switch # sh ip int brief

Vlan10	192.168.1.100	YES manual	up	up
Vlan20	192.168.2.100	YES manual	up	up

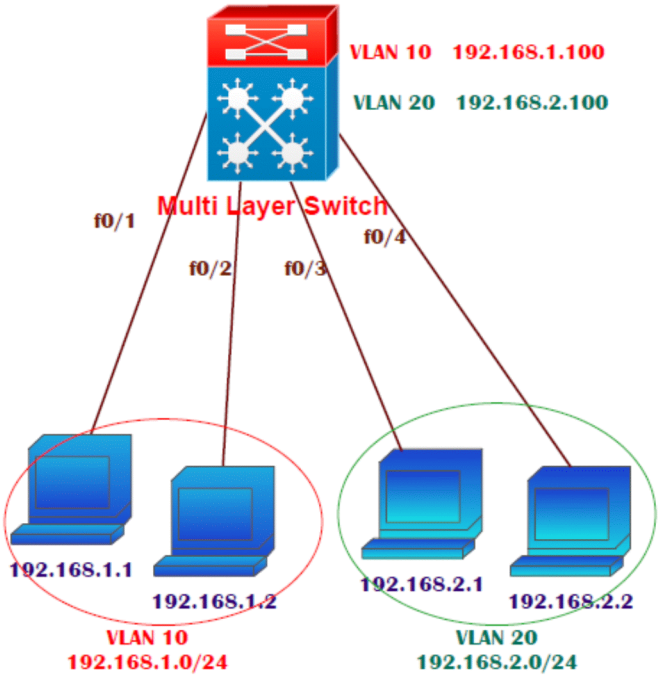
Layer 3 Port on MLS

```
Switch(config)#int fa0/20
Switch(config-if)#ip address 10.0.0.2  255.0.0.0
% Invalid input detected at '^' marker.

Switch(config-if)#no switchport
Switch(config-if)#ip address 10.0.0.2  255.0.0.0
```



- By default all the ports of any Multilayer Switch will be switchport (Layer 2)
- they don't understand IP addressing and just forward frames by identifying MAC address
- In our example we want f0/20 port of MLS as Router port (layer 3)
- To change the default Layer 2 port to a Router port we need to add command **"no switchport"**

LAB: Inter Vlan-Routing Using MLS



TASK:

- Create vlan and shift the ports as per the diagram
- create SVI (switch virtual interface) for each vlan and assing IP as per vlan addressing as per the diagram given
- Ensure that IP routing is enabled on Multilayer Switch
- verify connectivity between vlans (ping 192.168.1.1 ---192.168.2.1)

TASK: Create Vlan and Shift the Ports According To the Diagram

```
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#exit

Switch(config)#int range f0/1 - 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit

Switch(config)#int range f0/3 - 4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

TASK: Create SVI (Switch Virtual Interface) For Each Vlan

```
Switch (config)#int vlan 10
```

```
Switch(config-if)#ip address 192.168.1.100 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#int vlan 20
Switch(config-if)#ip address 192.168.2.100 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch # sh ip int brief

Vlan10          192.168.1.100   YES manual up                    up
Vlan20          192.168.2.100   YES manual up                    up
```

- The VLAN must be defined and active on the switch before the SVI can be used.
- The VLAN and the SVI are configured separately, even though they interoperate. Creating or configuring the SVI doesn't create or configure the VLAN; you still must define each one independently

```
Switch(config)#ip routing
```

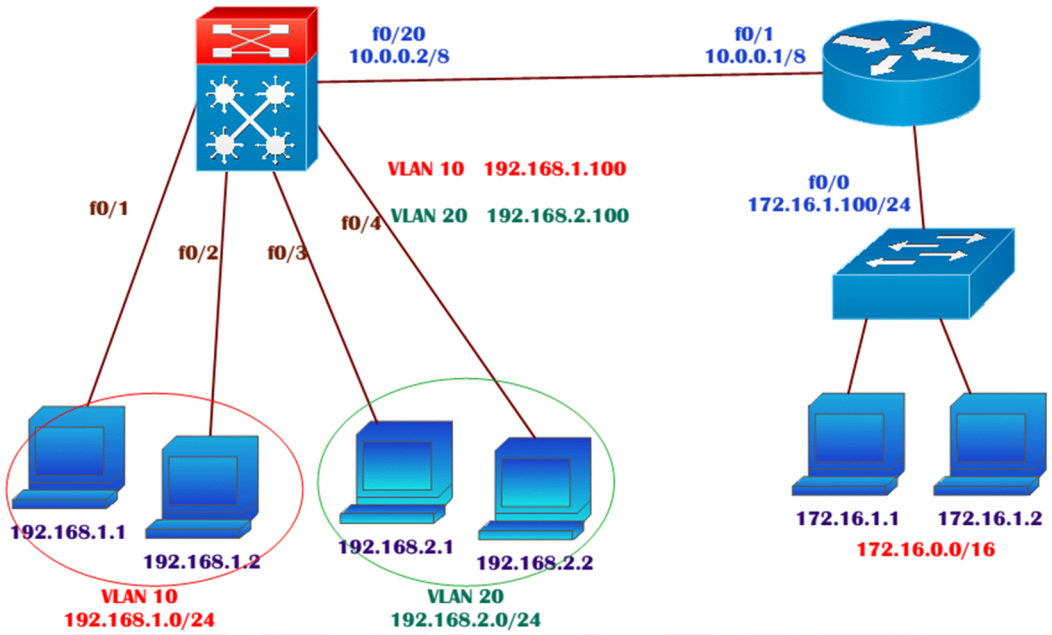
- Enable routing on the switch by using the ip routing command. Even if IP routing was previously enabled, this step ensures that it is activated.

Task : Verify Connectivity between VLANs (Ping 192.168.1.1 ---192.168.2.1)

```
PC>ipconfig

   IP Address.....: 192.168.1.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.1.100

PC>ping 192.168.2.1

   Pinging 192.168.2.1 with 32 bytes of data:
   Request timed out.
   Reply from 192.168.2.1: bytes=32 time=62ms TTL=127
   Reply from 192.168.2.1: bytes=32 time=125ms TTL=127
   Reply from 192.168.2.1: bytes=32 time=109ms TTL=127

PC>tracert 192.168.2.1

   Tracing route to 192.168.2.1 over a maximum of 30 hops:
    1   47 ms    63 ms    62 ms    192.168.1.100
    2   109 ms   125 ms   78 ms    192.168.2.1
```

TASK:

- Continue With The Previous Lab Configurations
- Add A Router Connecting To MLS as per the diagram (Assuming that there is a Wan Connection Between Router And MLS and they are different locations)



TASK: Configure IP addressing as per the Diagram on all Devices.

```
Router(config)#int f0/0
Router(config-if)#ip address 172.16.1.100 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#int f0/1
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#end

Router#sh ip int brief
      Interface              IP-Address      OK? Method Status                Protocol
       FastEthernet0/0       172.16.1.100    YES manual up                    up
       FastEthernet0/1       10.0.0.1        YES manual up                    up
```

On MLS

```
Switch(config)#int fa0/20
Switch(config-if)#ip address 10.0.0.2  255.0.0.0
```

^

% Invalid input detected at '^' marker.

- By default, every switch port on most Catalyst switch platforms is a Layer 2 interface, whereas every switch port on a Catalyst 6500 is a Layer 3 interface.
- If an interface needs to operate in a different mode, you must explicitly configure it.
- An interface is either in Layer 2 or Layer 3 mode, depending on the use of the switchport interface configuration command.
- You can display a port's current mode with the following command:
  - Switch# show interface type mod/num switchport
- If theSwitchport:line in the command output is shown as enabled, the port is in Layer 2 mode. If this line is shown as disabled, as in the following example, the port is inLayer 3 mode:

Switch# show interface gigabitethernet 0/1 switchport
Name: Gi0/1
Switchport: Disabled
Switch#

NOTE:

- By default all the ports ofany Multilayer Switch will be swithport (Layer 2)
- they don't understand IP addressing and just forward frames by identifying MAC address
- In our example we want f0/20 port of MLS as Router port (layer 3)
- To change the default Layer 2 port to a Router port we need to add command "no switchport"

Switch(config-if)#no switchport
Switch(config-if)#ip address 10.0.0.2 255.0.0.0

Switch #Sh ip int brief
FastEthernet0/20 10.0.0.2 YES manual up up

Switch#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/5/7 ms

MLS (3560)

Switch(config)#router rip
Switch(config-router)#version 2
Switch(config-router)#network 192.168.1.0
Switch(config-router)#network 192.168.2.0
Switch(config-router)#network 10.0.0.0
Switch(config-router)#no auto-summary
Switch(config-router)#end

ROUTER

```
Router(config)#router rip
Router(config-router)#ver 2
Router(config-router)#network 172.16.0.0
Router(config-router)#network 10.0.0.0
Router(config-router)#no auto-summary
Router(config-router)#end
```

```
Router#sh ip route
    C    10.0.0.0/8 is directly connected, FastEthernet0/1
    C    172.16.0.0/16 is directly connected, FastEthernet0/0
    R    192.168.1.0/24 [120/1] via 10.0.0.1, 00:00:01, FastEthernet0/1
    R    192.168.2.0/24 [120/1] via 10.0.0.1, 00:00:01, FastEth
```

```
Switch#sh ip route
    Gateway of last resort is not set
    C    10.0.0.0/8 is directly connected, FastEthernet0/20
    R    172.16.0.0/16 [120/1] via 10.0.0.2, 00:00:01, FastEthernet0/20
    C    192.168.1.0/24 is directly connected, Vlan10
    C    192.168.2.0/24 is directly connected, Vlan20
```

```
PC>ipconfig
    IP Address.....: 192.168.1.1
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 192.168.1.100
```

```
PC>ping 172.16.1.1
    Pinging 172.16.1.1 with 32 bytes of data:
    Request timed out.
    Reply from 172.16.1.1: bytes=32 time=125ms TTL=126
    Reply from 172.16.1.1: bytes=32 time=125ms TTL=126
    Reply from 172.16.1.1: bytes=32 time=125ms TTL=126
```

```
PC>tracert 172.16.1.1
    Tracing route to 172.16.1.1 over a maximum of 30 hops:
      1   31 ms     31 ms     32 ms     192.168.1.100
      2   63 ms     62 ms     62 ms     10.0.0.1
      3   109 ms    125 ms    125 ms    172.16.1.1
    Trace complete.
```

- Extended VLAN
- Voice VLAN

Extended VLAN

- Historically, Cisco Catalyst switches have supported only up to 1024 VLANs
- ISL uses 10-bit VLAN ID (upto 1024 Vlan)
- 802.1Q includes a 12-bit VLAN ID field (upto 4096 vlan)
- Cisco refers to the VLANs between 1025 and 4096 as extended-range VLANs.

Cisco Catalyst switches support extended-range VLANs under the following restrictions:

VTP cannot be used for VLAN management. (VTP must be configured in transparent mode or off

```
SW1(config)#vtp mode ?
  client      Set the device to client mode.
  off         Set the device to off mode.
  server      Set the device to server mode.
  transparent Set the device to transparent mode.
```

```
SW7(config)#vtp mode server
Setting device to VTP Server mode for VLANS.
```

```
SW7(config)#vlan 4000
SW7(config-vlan)#name sales
SW7(config-vlan)#exit
% Failed to create VLANs 4000
Extended VLAN(s) not allowed in current VTP mode.
%Failed to commit extended VLAN(s) changes.
```

Only Ethernet VLANs are supported.

```
SW1#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Gi0/1, Gi0/2
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

```
SW7(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
SW7(config)#vlan 4000
SW7(config-vlan)#name sales
SW7(config-vlan)#exit
```

```
SW7#sh vlan
VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                   Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                   Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                   Fa0/22, Gi0/1, Gi0/2
1002 fddi-default        act/unsup
1003 trcrf-default       act/unsup
1004 fddinet-default     act/unsup
1005 trbrf-default       act/unsup
4000 sales               active
```

- The spanning-tree extended system ID feature (also known as MAC address reduction) must be enabled.
- Enabled by default .You cannot disable the extended system ID feature.

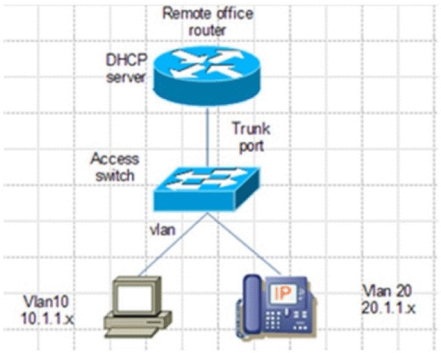
```
SW7#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN4000
Extended system ID      is enabled
Portfast Default        is disabled
PortFast BPDU Guard Default  is disabled
```

- SW7(config)#**spanning-tree extend system-id**

```
SW7(config)#no spanning-tree extend system-id
% Command "no spanning-tree extend system-id <cr>" was not accepted.
 extended system-id feature remains enabled due to extended VLAN existence.

SW7(config)#no vlan 4000

SW7(config)#no spanning-tree extend system-id
% Command "no spanning-tree extend system-id <cr>" was not accepted.
 This platform requires that the extended system-id feature remain enabled.
```

Voice VLAN

- voice VLAN feature enables access ports to carry IP voice traffic from an IP phone.
- switch can connect to IP Phone to carry IP voice traffic
- The Cisco IP Phone contains an integrated three-port 10/100 switch

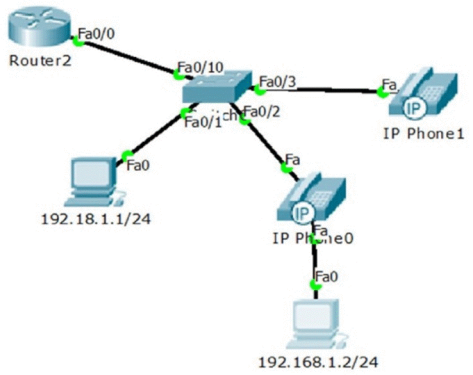


Default VLAN configuration :

- The voice VLAN feature is disabled by default.
- You should configure voice VLAN on switch access ports.
- The voice VLAN should be present and active on the switch for the IP phone to correctly communicate on the voice VLAN.
- Use the show vlan privileged EXEC command to see if the VLAN is present
- The Port Fast feature is automatically enabled when voice VLAN is configured.

Configuring Voice VLAN

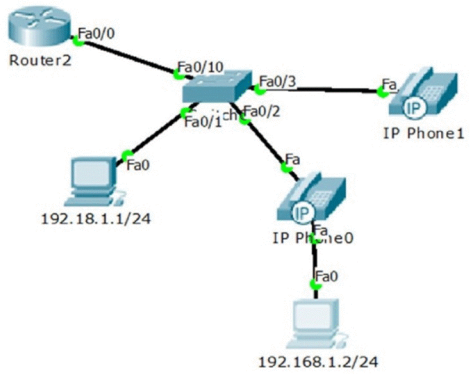
1. Create vlan 10 = DATA and Vlan 50 = VOICE
2. Assing Ports connecting to PC to Data vlan and IP phones to Voice VLAN



Configuring Voice VLAN (contd)

Create vlan 10 = DATA and Vlan 50 = VOICE

```
Switch(config)#vlan 10
Switch(config-vlan)#name DATA
Switch(config-vlan)#exit

Switch(config)#vlan 50
Switch(config-vlan)#name VOICE
Switch(config-vlan)#exit
```

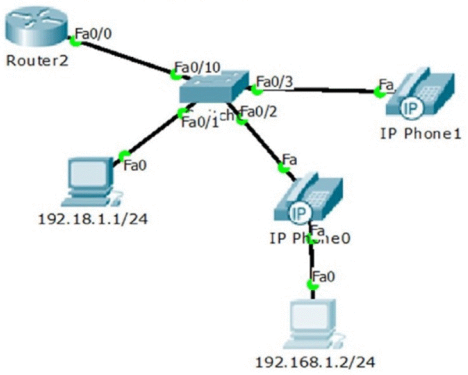


Configuring Voice VLAN (contd)

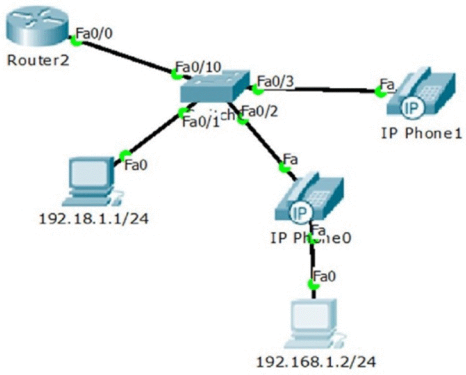
Assign Ports connecting to PC to Datav lan and IP phones to Voice VLAN

```
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit

Switch(config)# int f0/3
Switch(config-if)#  switchport mode access
Switch(config-if)#switchport voice  vlan 50
Switch(config-if)#exit
```

```
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport voice vlan 50
Switch(config-if)#end
```



Configuring Voice VLAN (contd)

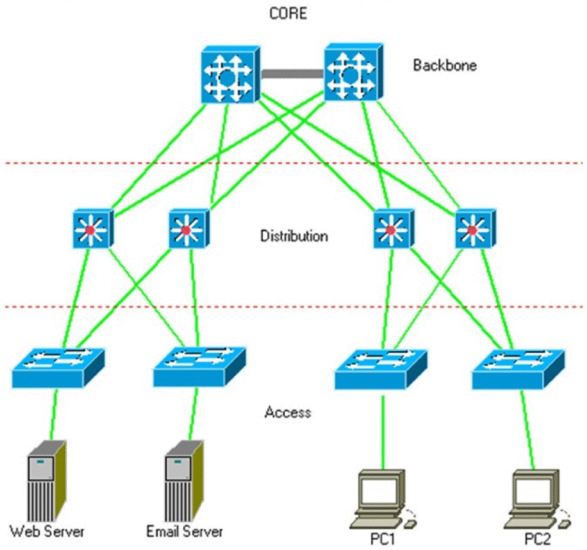



```
Switch#show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
10   DATA                              active    Fa0/1, Fa0/2
50   VOICE                             active    Fa0/2, Fa0/3
```

VTP

VLAN TRUNKING PROTOCOL

- VTP is a CISCO proprietary protocol
- used to share the VLAN configurations with multiple switches and to maintain consistency throughout that network.

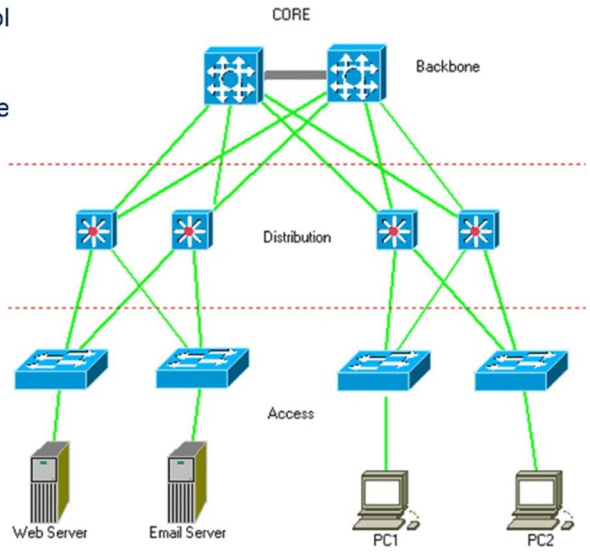


VTP

- VTP manages the addition, deletion, and renaming of VLANs across the network from a central point of control
- Information will be passed only if switches connected with Fast Etherne or higher ports.
- Also must be trunk links

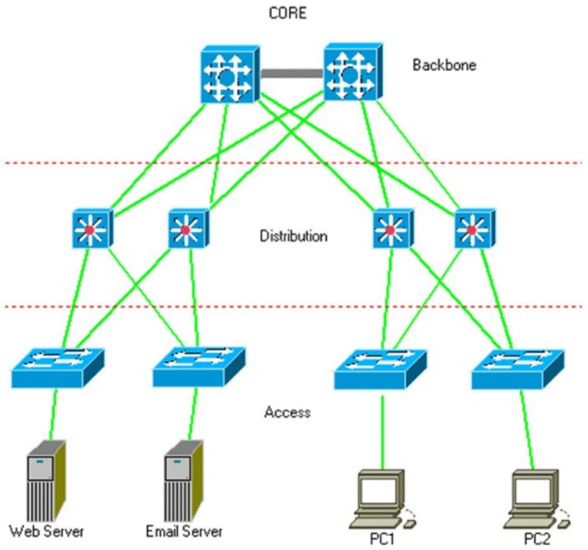
Note:

- Switches Should be configure with same Domain.
- Domain are not Case sensitive.



VTP MODES

1. Server Mode
2. Client mode
3. Transparent mode

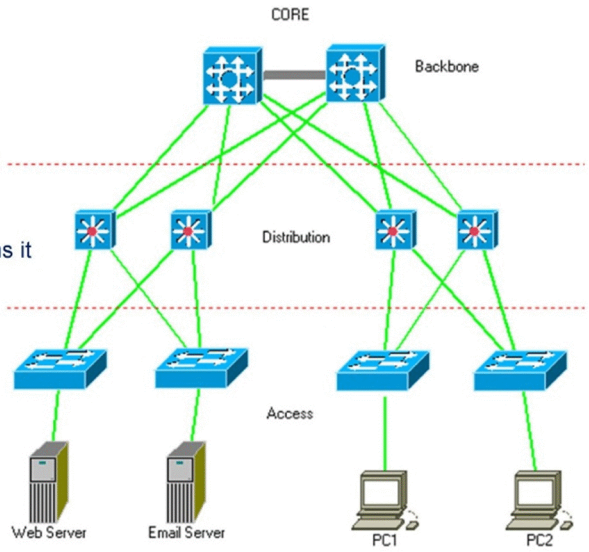


Server Mode

- Default mode
- Creates, modifies, and deletes VLANs
- Synchronizes VLAN configurations
- Sends and forwards advertisements
- Saves configuration in NVRAM

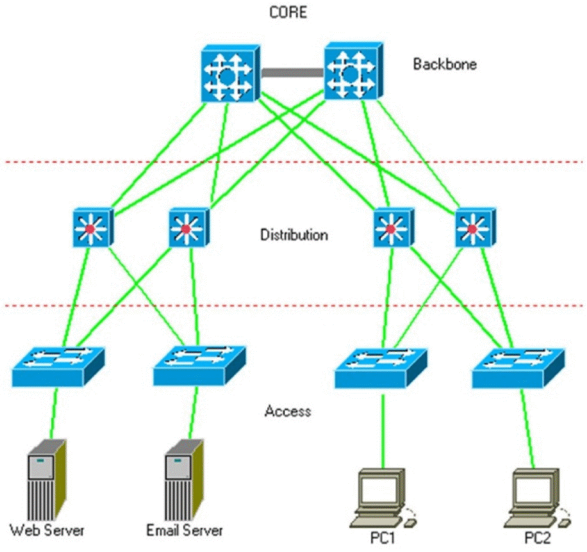
Client Mode

- cannot Add , Modify and Delete its VLAN configurations
- Doesn't store its VLAN configuration information in the NVRAM. Instead , learns it from the server every time it boots up
- Forwards advertisements
- Synchronizes VLAN configurations
- Do not save in NVRAM

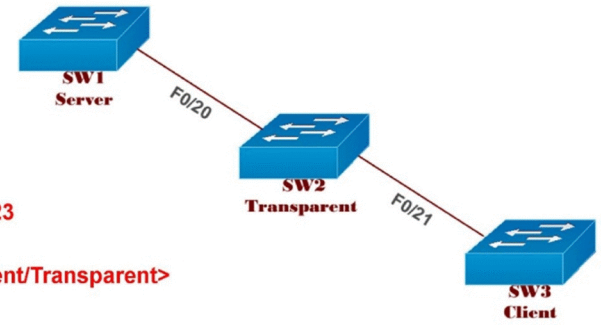


Transparent Mode

- can Add , Modify and Delete VLAN configurations.
- Does not synchronize VLAN configurations
- Forwards advertisements
- Saves configuration in NVRAM



Configuring VTP



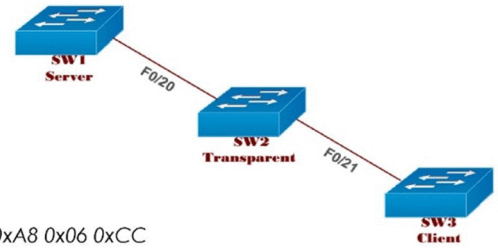

```
Switch(Config)# VTP domain CCIE
Switch(Config)# Vtp password cisco123
Switch(Config)# Vtp version 2
Switch(Config)# Vtp mode <server/Client/Transparent>
Switch(Config)# Vtp pruning

SW1#sh vtp status
SW1#sh vtp  password
```

- VTP is off by default
- VTP once enabled uses version 1 only

Configuration Revision Number

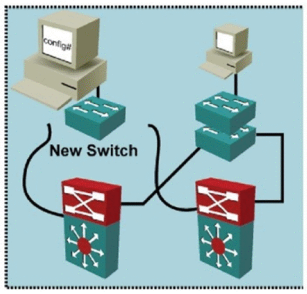
- VTP switches use an index called the VTP configuration revision number to keep track of the most recent information.
- The VTP advertisement process always starts with configuration revision number 0 (zero).
- When subsequent changes are made on a VTP server, the revision number is incremented before the advertisements are sent.

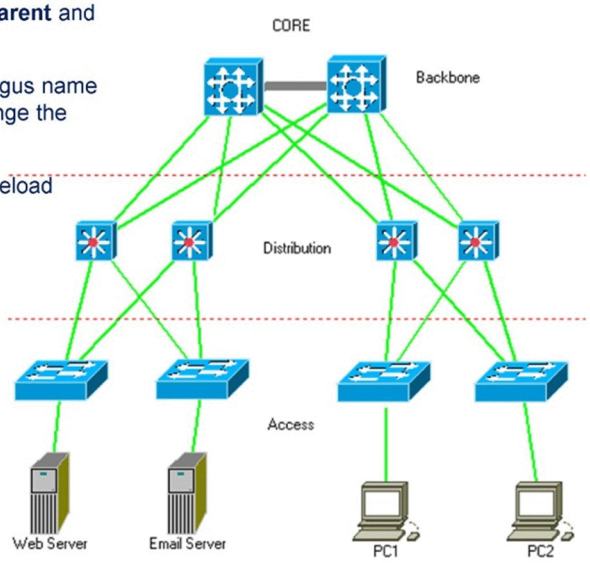
```
SW-3#sh vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x86 0x22 0x83 0x8E 0x23 0xA8 0x06 0xCC
Configuration last modified by 0.0.0.0 at 3-1-93 00:07
```



Before Adding a Switch to an Existing VTP Domain , Ensure a new switch has VTP revision is 0 before adding it to a network.

- Change the switch's **VTP mode to transparent** and then change the mode **back to server.**
- Change the **switch's VTP domain** to a bogus name (a nonexistentVTP domain), and then change the VTP domain back to the original name.
- **Delete Vlan.dat file** inside the Flash and reload

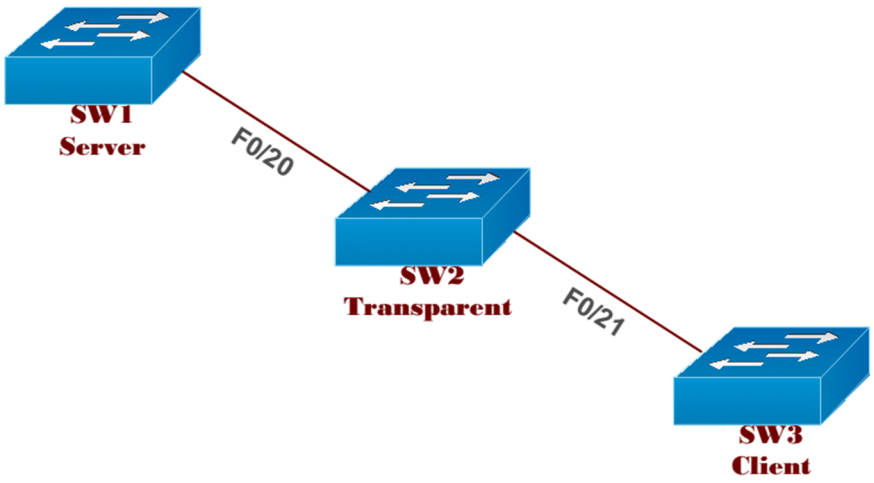




VTP Versions

VTP version 1	VTP Version 2
Supports only one VTP domain	Support multiple VTP domain
Check for domain name (if matches then only forward VTP messages)	No check
More consistent check (add more overhead)	Check for consistency ,whenever new information is added
NO	Support for Token ring VLAN

LAB: VTP



TASK:

1) Configure the links between Switches as Trunks. (vtp advertisements are send only on trunk ports)
2) Configure VTP on all switches as per thegiven modes in the Diagram above.
3) To verify VTP
   a. Create vlans on server and verify on client and transparent switch
   b. Create vlans on transparent switch and verify on client and server

On SW1 (SERVER)

```
SW-1(config)#int f0/20
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#switchport trunk encapsulation dot1q
```

SW2 (TRANSPARENT)

```
SW2(config)#int range fa0/20 - 21
SW-2(config-if)#switchport mode trunk
SW-2(config-if)#switchport trunk encapsulation dot1q
```

SW3 (CLIENT)

```
SW3(config)#int f0/21
SW-3(config-if)#switchport mode trunk
SW-3(config-if)#switchport trunk encapsulation dot1q
```

```
SW1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
```

SW2#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1
Fa0/21	on	802.1q	trunking	1

SW-3#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/21	on	802.1q	trunking	1

TASK:

- Configure VTP on all switches as per thegiven modes in the Diagram above.
- (SW1 –SERVER. SW2 – TRANSPARENT, SW3 – CLIENT)

Make Sure that Domain name (case-sensitive) / password / version must match on all switches for sending and receiving VTP Messages

SW1

```
SW-1(config)#vtp domain CCNP
SW-1(config)#vtp password cisco123
SW-1(config)#vtp version 2
SW-1(config)#vtp mode server
```

SW2

```
SW-2(config)#vtp domain CCNP
SW-2(config)#vtp password cisco123
SW-2(config)#vtp version 2
SW-2(config)#vtp mode transparent
```

SW3

```
SW-1(config)#vtp domain CCNP
SW-1(config)#vtp password cisco123
SW-1(config)#vtp version 2
SW-1(config)#vtp mode client
```

SW1#sh vtp status

```
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
```

MD5 digest : 0x86 0x22 0x83 0x8E 0x23 0xA8 0x06 0xCC
Configuration last modified by 0.0.0.0 at 3-1-93 00:07:33
Local updater ID is 0.0.0.0 (no valid interface found

SW1#sh vtp password
VTP Password: cisco123

The current VTP parameters for a management domain can be displayed using the show vtp statuscommand

SW-3#sh vtp status
VTP Version : 2
Configuration Revision : 2
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Client
VTP Domain Name : CCNP
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0x86 0x22 0x83 0x8E 0x23 0xA8 0x06 0xCC
Configuration last modified by 0.0.0.0 at 3-1-93 00:07

To verify VTP

- Create vlans on server and verify on client and transparent switch
- Create vlans on transparent switch and verify on client and server

SW1

SW-1(config)#vlan 10
SW-1(config-vlan)#vlan 20
SW-1(config-vlan)#vlan 30

SW-1(config-vlan)#vlan 40
SW-1(config-vlan)#name sales

SW-1(config-vlan)#vlan 50
SW-1(config-vlan)#name marketing

R1#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
			Fa0/5, Fa0/6, Fa0/7, Fa0/8
			Fa0/9, Fa0/10, Fa0/11, Fa0/12

```
                                          Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                          Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                          Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                          Gig1/2
10   VLAN0010                             active
20   VLAN0020                             active
30   VLAN0030                             active
40   sales                                active
50   marketing                            active
1002 fddi-default                         act/unsup
1003 token-ring-default                   act/unsup
1004 fddinet-default                      act/unsup
1005 trnet-default                        act/unsup
```

SW-3#sh vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                 Gig1/2
10   VLAN0010                                    active
20   VLAN0020                                    active
30   VLAN0030                                    active
40   sales                                       active
50   marketing                                   active
```

Sw-2#sh vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/22
                                                 Fa0/23, Fa0/24, Gig1/1, Gig1/2
1002 fddi-default                         act/unsup
1003 token-ring-default                   act/unsup
1004 fddinet-default                      act/unsup
1005 et-default                           act/unsup
```

You don't see any vlan on the transparent mode switch as the transparent will not synchronize the vlan information from any other Swithces but still forward the Vlan information.

```
Sw-2(config)#vlan 100
Sw-2(config-vlan)#vlan 200
Sw-2(config-vlan)#vlan 300
Sw-2(config-vlan)#end

SW2 #sh vlan
        VLAN Name                              Status    Ports
        ---- --------------------------------- --------- -------------------------------
        1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                         Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                         Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                         Fa0/17, Fa0/18, Fa0/19, Fa0/22
                                                         Fa0/23, Fa0/24
        100  VLAN0100                          active
        200  VLAN0200                          active
        300  VLAN0300                          active
        1002 fddi-default                      act/unsup

Sw1#sh vlan
        VLAN Name                              Status    Ports
        ---- --------------------------------- --------- -------------------------------
        1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                         Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                         Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                         Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                         Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                         Gig1/2
        10   VLAN0010                          active
        20   VLAN0020                          active
        30   VLAN0030                          active
        40   VLAN0040                          active
        1002 fddi-default                      act/unsup
        1003 token-ring-default                act/unsup
        1004 fddinet-default                   act/unsup
        1005 trnet-default                     act/unsup
```

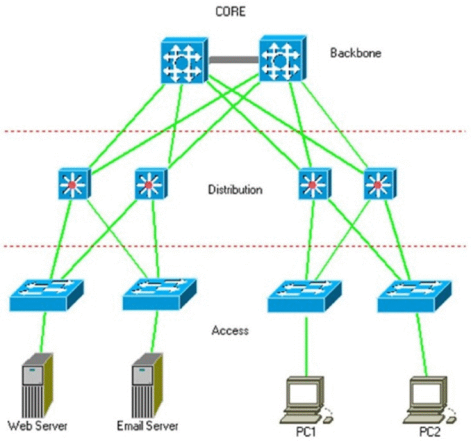
```
SW3 # sh vlan
        VLAN Name                              Status    Ports
        ---- --------------------------------- --------- -------------------------------
        1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                         Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                         Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                         Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                         Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                         Gig1/2
        10   VLAN0010                          active
        20   VLAN0020                          active
        30   VLAN0030                          active
        40   VLAN0040                          active
        1002 fddi-default                      act/unsup
        1003 token-ring-default                act/unsup
        1004 fddinet-default                   act/unsup
        1005 trnet-default                     act/unsup
```

- You can see the vlans created on the transparent switch are not present in any of the other switches (SW1 or SW3) because the switch in transparent mode will not synchronize the vlan information
- Revision number for switches in the transparent mode will be always ZERO.

```
Sw-2#sh vtp status
        VTP Version                     : 2
        Configuration Revision          : 0
        Maximum VLANs supported locally : 255
        Number of existing VLANs        : 8
        VTP Operating Mode              : Transparent
        VTP Domain Name                 : CCNP
        VTP Pruning Mode                : Disabled
        VTP V2 Mode                     : Enabled
        VTP Traps Generation            : Disabled
        MD5 digest                      : 0xB7 0x9D 0xA5 0xEF 0xDE 0x56 0xC5 0xCF
        Configuration last modified by 0.0.0.0 at 3-1-93 00:07
```

VTP version 3

- Protection against data overwrites. (fix the configuration revision number higher udpating)
  - Primary server can only make changes (only one)
- Support for VLAN numbers up to 4096
- Can also advertise
  - advertise Extended vlan information (1006- 4094)
  - Private vlan information
  - Mst configuration
- Option of clear text or hidden password protection
- VTP can be disabled globally or interface level

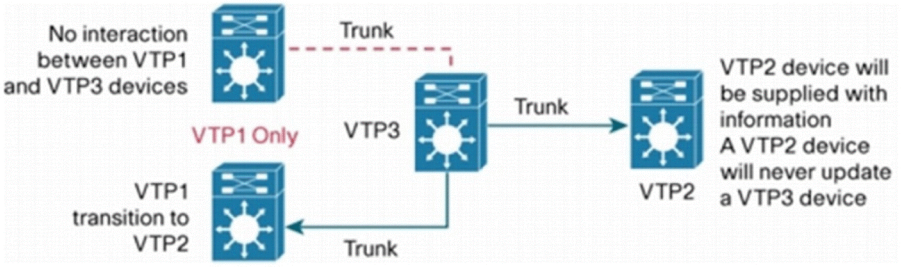



```
Catalyst6500-1(config)# vtp version 3
Cannot set the version to 3 because domain name is not configured.
```

VTP Roles Versus Functions and Behavior

MST - VTP3	Relay/Process	Configure	Save
PRIMARY SRV	Yes	Yes	Yes
SECONDARY SRV	Yes	No	Yes
CLIENT	Yes	No	No
TRANSPARENT	Yes	Yes	Yes
OFF	No	Yes	Yes

VTP3 interoperates with VTP version 2 but not VTP version 1.



VTP version 3 configuration is mostly performed in global configuration mode.

Catalyst6500-1(config)# **vtp ?**

domain	Set the name of the VTP administrative domain.
file	Configure IFS filesystem file where VTP configuration is stored.
interface	Configure interface as the preferred source for the VTP IP updater address.
mode	Configure VTP device mode
Password	Set the password for the VTP administrative domain
pruning	Set the administrative domain to permit pruning
version	Set the administrative domain to VTP version

LAB: VTP version 3

TASK:

- Configure f0/24 port of sw1/Sw2 as Trunk ports.
- Configure VTP version 3 using following parameters:
- Domain name : NOA
- Password hidden : noa123

```
SW1(config)#int f0/24
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit

SW2(config)#int f0/24
SW2(config-if)#  switchport trunk encapsulation dot1q
SW2(config-if)#  switchport mode trunk
SW2(config-if)#end

SW2#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/24      1-4094
Port        Vlans allowed and active in management domain
Fa0/24      1
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      none

SW2#sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0023.041c.5e00
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
```

```
---------------
VTP Operating Mode              : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                  0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC
```

SW1#sh vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                                 Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

SW1(config)#vtp domain NOA
SW1(config)#vtp password noa123
SW1(config)#vtp version 3

SW2(config)#vtp domain NOA
SW2(config)#vtp password noa123
SW2(config)#vtp version 3
SW2(config)#end

SW2#sh vtp status

```
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : NOA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0023.041c.5e00

Feature VLAN:
--------------
VTP Operating Mode              : Server
Number of existing VLANs          : 5
```

```
Number of existing extended VLANs: 0
Maximum VLANs supported locally   : 1005
Configuration Revision            : 0
Primary ID                        : 0000.0000.0000
Primary Description               :
MD5 digest                        :
Feature MST:
----------
VTP Operating Mode                : Transparent
Feature UNKNOWN:
----------
VTP Operating Mode                : Transparent
```

SW2#sh vtp password

```
VTP Password: noa123
```

TASK: Configure Switches to ensure that the password should be seen.

SW2#sh vtp password

```
VTP Password: noa123
```

SW2(config)#vtp password noa123 ?

```
  hidden  Set the VTP password hidden option
  secret  Specify the vtp password in encrypted form
  <cr>
```

SW2(config)#vtp password noa123 hidden

SW1(config)#vtp password noa123 hidden
SW1(config)#end

SW1#sh vtp password

```
VTP Password: D09CEE53D89CFC68C33886FCF64BDC1A
```

TASK:

- Create vlan 10,20,30,40 on SW1 and ensure that it synchonises on both switches:
- Configure SW1 to be primary switch to update the database.

SW1(config)#vlan 10

```
VTP VLAN configuration not allowed when device is not the primary server for vlan database.
```

SW1#vtp primary vlan

```
This system is becoming primary server for feature vlan
Enter VTP Password:
```

```
No conflicting VTP3 devices found.
Do you want to continue? [Confirm]

*Mar  1 00:11:59.054: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: 0022.be79.2e00 has  become the
primary server for the VLAN VTP feature

SW1#sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : NOA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0022.be79.2e00

Feature VLAN:
--------------
VTP Operating Mode              : Primary Server
Number of existing VLANs        : 5
Number of existing extended VLANs : 0
Maximum VLANs supported locally   : 1005
Configuration Revision          : 1
Primary ID                      : 0022.be79.2e00
Primary Description             : SW1
MD5 digest                      : 0x1E 0xA7 0x8E 0x46 0x94 0xBE 0x95 0xA5
                                  0x9D 0x6E 0xD5 0x69 0x72 0xEF 0x03 0xD0

Feature MST:
--------------
VTP Operating Mode              : Transparent

Feature UNKNOWN:
--------------
VTP Operating Mode              : Transparent

SW1(config)#vlan 10,20,30,40
SW1(config-vlan)#end

SW1#sh vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
```

```
                                    Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                    Gi0/2
10   VLAN0010                       active
20   VLAN0020                       active
30   VLAN0030                       active
40   VLAN0040                       active
1002 fddi-default                   act/unsup
1003 trcrf-default                  act/unsup
1004 fddinet-default                act/unsup
1005 trbrf-default                  act/unsup
```

SW2#sh vlan brief

```
VLAN Name                          Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                    Gi0/2
10   VLAN0010                       active
20   VLAN0020                       active
30   VLAN0030                       active
40   VLAN0040                       active
1002 fddi-default                   act/unsup
1003 trcrf-default                  act/unsup
1004 fddinet-default                act/unsup
1005 trbrf-default                  act/unsup
```

SW2#sh vtp status

```
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : NOA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0023.041c.5e00

Feature VLAN:
--------------
VTP Operating Mode              : Server
Number of existing VLANs        : 9
Number of existing extended VLANs : 0
Maximum VLANs supported locally   : 1005
```

```
Configuration Revision          : 3
Primary ID                      : 0022.be79.2e00
Primary Description             : SW1
MD5 digest                      : 0xBF 0x17 0x16 0xA3 0x73 0x09 0x0F 0x2E
                                  0xEC 0x19 0x4F 0xCA 0x13 0xEE 0xD4 0x79

Feature MST:
--------------
VTP Operating Mode              : Transparent

Feature UNKNOWN:
--------------
VTP Operating Mode              : Transparent
```

TASK: Create extended vlan 2000 - 2001 on SW1

```
SW1(config)#vlan 2000-2001
SW1(config-vlan)#end

SW1#sh vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                                 Gi0/2
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
40   VLAN0040                          active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
2000 VLAN2000                          active
2001 VLAN2001                          active

SW2#sh vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
```

```
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                  Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                  Gi0/2
10   VLAN0010                     active
20   VLAN0020                     active
30   VLAN0030                     active
40   VLAN0040                     active
1002 fddi-default                 act/unsup
1003 trcrf-default                act/unsup
1004 fddinet-default              act/unsup
1005 trbrf-default                act/unsup
2000 VLAN2000                     active
2001 VLAN2001                     active
```

TASK: Promote SW2 to be the primary server and create vlan 3000-3005 on SW2

SW2#vtp primary vlan

```
This system is becoming primary server for feature vlan
Enter VTP Password:
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
```

*Mar 1 00:15:16.556: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: 0023.041c.5e00 has become the primary server for the VLAN VTP feature

SW2#sh vtp status

```
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : NOA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0023.041c.5e00

Feature VLAN:
--------------
VTP Operating Mode              : Primary Server
Number of existing VLANs        : 9
Number of existing extended VLANs : 2
Maximum VLANs supported locally   : 1005
Configuration Revision          : 4
Primary ID                      : 0023.041c.5e00
```

```
    Primary Description           : SW2
    MD5 digest                    : 0x1D 0x11 0xA3 0x1F 0x76 0x7C 0xE7 0xD7
                                    0x1B 0x28 0xB9 0xBD 0xF0 0x71 0x1E 0xBC
    Feature MST:
    ----------
    VTP Operating Mode            : Transparent
     Feature UNKNOWN:
    ----------
    VTP Operating Mode            : Transparent

SW1#sh vtp status
    VTP Version capable           : 1 to 3
    VTP version running           : 3
    VTP Domain Name               : NOA
    VTP Pruning Mode              : Disabled
    VTP Traps Generation          : Disabled
    Device ID                     : 0022.be79.2e00

    Feature VLAN:
    ----------
    VTP Operating Mode            : Server
    Number of existing VLANs      : 9
    Number of existing extended VLANs : 2
    Maximum VLANs supported locally   : 1005
    Configuration Revision        : 4
    Primary ID                    : 0023.041c.5e00
    Primary Description           : SW2
    MD5 digest                    : 0x1D 0x11 0xA3 0x1F 0x76 0x7C 0xE7 0xD7
                                    0x1B 0x28 0xB9 0xBD 0xF0 0x71 0x1E 0xBC
    Feature MST:
    ----------
    VTP Operating Mode            : Transparent

    Feature UNKNOWN:
    ----------
    VTP Operating Mode            : Transparent

SW2(config)#vlan 3000-3001
SW2(config-vlan)#end

SW2#sh vlan brief
    VLAN Name                     Status    Ports
    ---- -------------------------------- --------- -------------------------------
    1    default                  active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
```

```
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                  Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                  Gi0/2
10   VLAN0010                     active
20   VLAN0020                     active
30   VLAN0030                     active
40   VLAN0040                     active
1002 fddi-default                 act/unsup
1003 trcrf-default                act/unsup
1004 fddinet-default              act/unsup
1005 trbrf-default                act/unsup
2000 VLAN2000                     active
2001 VLAN2001                     active
3000 VLAN3000                     active
3001 VLAN3001                     active
```

TASK:

- Cofigure MSTP on SW1 and ensure that SW2 should also synchronise the MSTP configuration information.

SW1#sh spanning-tree mst configuration

```
% Switch is not in mst mode
Name      []
Revision  0     Instances configured 1

Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
------------------
```

SW1#vtp primary mst

System can become primary server for Mst feature only when configured as a server

SW1#sh vtp status

```
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : NOA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0022.be79.2e00

Feature VLAN:
```

```
---------------
VTP Operating Mode              : Server
Number of existing VLANs        : 9
Number of existing extended VLANs : 4
Maximum VLANs supported locally   : 1005
Configuration Revision          : 5
Primary ID                      : 0023.041c.5e00
Primary Description             : SW2
MD5 digest                      : 0xB0 0xFA 0x11 0x95 0x0F 0xA9 0xF3 0x58
                                  0x38 0x96 0xDE 0x1B 0x26 0x37 0x8F 0xD9
Feature MST:
---------------
VTP Operating Mode              : Transparent

Feature UNKNOWN:
---------------
VTP Operating Mode              : Transparent
```

```
SW1(config)#vtp mode server mst
Setting device to VTP Server mode for MST.
SW1(config)#end
```

```
SW1#vtp primary mst
    This system is becoming primary server for feature  mst
    Enter VTP Password:
    No conflicting VTP3 devices found.
    Do you want to continue? [confirm]
```

```
*Mar  1 00:21:20.554: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: 0022.be79.2e00 has become the primary server for the MST VTP feature
```

```
SW1#sh vtp status
    VTP Version capable             : 1 to 3
    VTP version running             : 3
    VTP Domain Name                 : NOA
    VTP Pruning Mode                : Disabled
    VTP Traps Generation            : Disabled
    Device ID                       : 0022.be79.2e00

    Feature VLAN:
    --------------
    VTP Operating Mode              : Server
    Number of existing VLANs        : 9
    Number of existing extended VLANs : 4
```

```
Maximum VLANs supported locally   : 1005
Configuration Revision            : 5
Primary ID                        : 0023.041c.5e00
Primary Description               : SW2
MD5 digest                        : 0xB0 0xFA 0x11 0x95 0x0F 0xA9 0xF3 0x58
                                    0x38 0x96 0xDE 0x1B 0x26 0x37 0x8F 0xD9
Feature MST:
--------------
VTP Operating Mode                : Primary Server
Configuration Revision            : 1
Primary ID                        : 0022.be79.2e00
Primary Description               : SW1
MD5 digest                        : 0x86 0x43 0x4F 0x9D 0x7C 0x8F 0x0F 0xEB
                                    0x1F 0x25 0xD2 0x5A 0x55 0x98 0xE1 0x19

Feature UNKNOWN:
--------------
VTP Operating Mode                : Transparent
```

```
SW2(config)#vtp mode client mst
Setting device to VTP Client mode for MST.

SW1(config)#spanning-tree mode mst
SW1(config)#spanning-tree mst configuration
SW1(config-mst)#name CCIE
SW1(config-mst)#revision 1
SW1(config-mst)#instance 1 vlan 10,20
SW1(config-mst)#instance 2 vlan 30,40
SW1(config-mst)#exit

SW1#sh spanning-tree mst configuration
    Name      [CCIE]
    Revision  1     Instances configured 3

    Instance  Vlans mapped
    --------  ---------------------------------------------------------------------
    0         1-9,11-19,21-29,31-39,41-4094
    1         10,20
    2         30,40
    ---------------------------------------------------------------------------

SW2#sh spanning-tree mst configuration
    % Switch is not in mst mode
    Name      [CCIE]
```

```
Revision  1     Instances configured 3

Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-9,11-19,21-29,31-39,41-4094
1         10,20
2         30,40
---------------------------------------------------------------------------
```

SW2(config)#spanning-tree mode mst

SW2#sh spanning-tree mst configuration

```
Name      [CCIE]
Revision  1     Instances configured 3

Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-9,11-19,21-29,31-39,41-4094
1         10,20
2         30,40
---------------------------------------------------------------------------
```

TASK:

- Configure Private VLAN information on SW2 and verify VTP synchronizing private vlan information.

SW2(config)#vlan 10
SW2(config-vlan)#vlan 100
SW2(config-vlan)#vlan 200
SW2(config-vlan)#exit

SW2(config)#vlan 10
SW2(config-vlan)#private-vlan primary
SW2(config-vlan)#exit

SW2(config)#vlan 100
SW2(config-vlan)#private-vlan isolated
SW2(config-vlan)#exit

SW2(config)#vlan 200
SW2(config-vlan)#private-vlan community
SW2(config-vlan)#exit

SW2(config)#vlan 10
SW2(config-vlan)#private-vlan primary
SW2(config-vlan)#private-vlan association 100,200

SW2(config-vlan)#exit

SW2#sh vlan private-vlan

```
Primary Secondary Type            Ports
------- --------- ----------------- ------------------------------------------
10      100       isolated
10      200       community
```

SW1#sh vlan private-vlan

```
Primary Secondary Type            Ports
------- --------- ----------------- ------------------------------------------
10      100       isolated
10      200       community
```

SW1# sh vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                                 Gi0/2
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
40   VLAN0040                          active
100  VLAN0100                          active
200  VLAN0200                          active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
2000 VLAN2000                          active
2001 VLAN2001                          active
3000 VLAN3000                          active
3001 VLAN3001                          active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
```

```
30   enet  100030     1500  -      -      -        -    -       0     0
40   enet  100040     1500  -      -      -        -    -       0     0
100  enet  100100     1500  -      -      -        -    -       0     0
200  enet  100200     1500  -      -      -        -    -       0     0
1002 fddi  101002     1500  -      -      -        -    -       0     0
1003 trcrf 101003     4472  1005   3276   -        -    srb     0     0
1004 fdnet 101004     1500  -      -      -        ieee -       0     0
1005 trbrf 101005     4472  -      -      15       ibm  -       0     0
2000 enet  102000     1500  -      -      -        -    -       0     0
2001 enet  102001     1500  -      -      -        -    -       0     0
3000 enet  103000     1500  -      -      -        -    -       0     0
3001 enet  103001     1500  -      -      -        -    -       0     0

VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
1003 7       7       off

Remote SPAN VLANs
------------------------------------------------------------------------------
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      100       isolated
10      200       community
```

TASK: Configure SW1 to disable VTP globally or interace level on f0/23

```
SW1#  sh vtp status
    VTP Version capable             : 1 to 3
    VTP version running             : 3
    VTP Domain Name                 : NOA
    VTP Pruning Mode                : Disabled
    VTP Traps Generation            : Disabled
    Device ID                       : 0022.be79.2e00

    Feature VLAN:
    --------------
    VTP Operating Mode              : Server
    Number of existing VLANs        : 11
    Number of existing extended VLANs : 4
    Maximum VLANs supported locally   : 1005
    Configuration Revision          : 12
    Primary ID                      : 0023.041c.5e00
    Primary Description             : SW2
    MD5 digest                      : 0xEE 0x2B 0x19 0x0E 0xD1 0xBD 0xF9 0x96
```

0x34 0xE8 0x14 0xD1 0x68 0xB1 0xF2 0xB3

Feature MST:

VTP Operating Mode : Primary Server
Configuration Revision : 2
Primary ID : 0022.be79.2e00
Primary Description : SW1
MD5 digest : 0x03 0x46 0xEB 0xBA 0x16 0x90 0xAC 0x22
0xB3 0x6F 0x31 0x99 0x5C 0x0E 0x9B 0xF8

Feature UNKNOWN:

VTP Operating Mode : Transparent

TASK: Disable VTP on SW1 using Mode off:

```
SW1(config)#vtp mode off vlan
    Setting device to VTP Off mode for VLANS.
SW1(config)#vtp mode off mst
    Setting device to VTP Off mode for MST.
```

TASK : Re-eable VTP on sw1 (vlan and msT) and Disable VTP only on interface f0/23.

```
SW1(config)#vtp mode server vlan
    Setting device to VTP Server mode for VLANS.

SW1(config)#vtp mode server mst
    Setting device to VTP Server mode for MST.

SW1(config)#int f0/23
SW1(config-if)#no vtp
SW1(config-if)#end
```

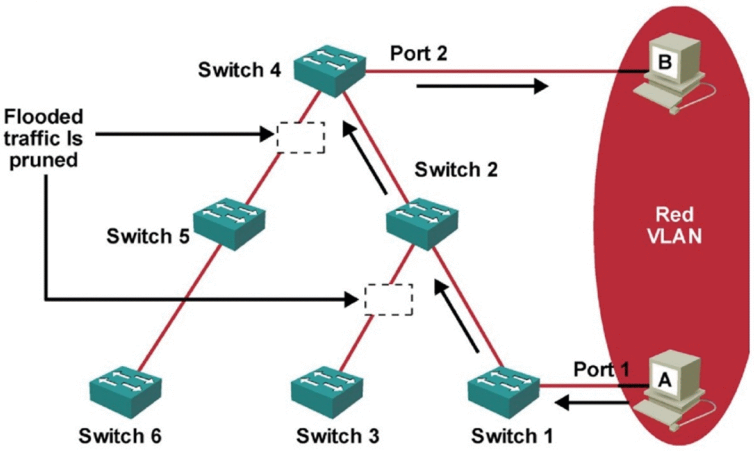
TASK: Create vlan 199 and enable RSPAN and ensure that it synchronises this information as well

```
SW2(config)#vlan 199
SW2(config-vlan)#remote-span
SW2(config-vlan)#end

SW2#sh vlan remote-span
    Remote SPAN VLANs
    ------------------------------------------------------------------------
    199
```

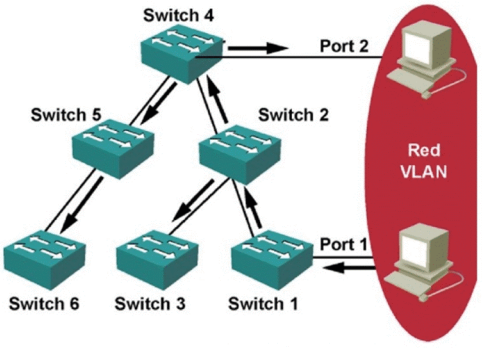
```
SW1#sh vlan remote-span
Remote SPAN VLANs
------------------------------------------------------------------------------
199
```

VTP pruning

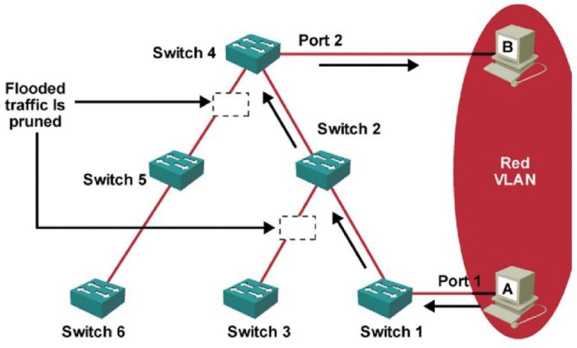
- VTP pruning makes more efficient use of trunk bandwidth by reducing unnecessary flooded traffic.
- Broadcast and unknown unicast frames on a VLAN are forwarded over a trunk link only if the switch on the receiving end of the trunk has ports in that VLAN.
- Preserves bandwidth by configuring it to reduce the amount of broadcasts, multicasts, and unicast packets.



- Uses bandwidth more efficiently by reducing unnecessary flooded traffic
- Example: Station A sends broadcast; broadcast flooded only toward any switch with ports assigned to the red VLAN



Pruning Disabled

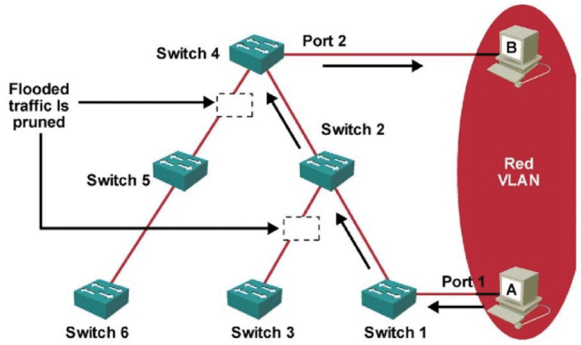


Pruning Enabled

- Enabling pruning on a VTP server, enables it for the entire domain.
- By default, VLANs 2 through 1005 are pruning-eligible, but VLAN 1 can never prune because it's an administrative VLAN.
- All VLANs by default are prune eligible, which means that all VLANs can be pruned by this protocol.
- To block specific VLANs from the pruning mechanism, we must use the **switchport trunk pruning vlan** command.

server(Config)# **Vtp pruning**

```
Rack1SW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
VTP Operating Mode              : Server
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
```



Verify VTP pruning

```
Switch1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,1002,1003,1004,1005

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,1002,1003,1004,1005
```

```
Rack1SW1#show interface fa0/16 pruning

Port        Vlans pruned for lack of request by neighbor
Fa0/16      7-8,10,22,58,67,146

Port        Vlan traffic requested of neighbor
Fa0/16      1,5,7-10,22,43,58,67,79,146
```

VTP prune eligible list

switchport trunk pruning vlan {**add** *vlan-list* | **all** | **except** *vlan-list* | **remove** *vlan-list*}

- To configure the VLAN pruning-eligible list for ports in trunking mode.
- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list.
- VLANs that are pruning-ineligible receive flooded traffic.

Switch(config-if)**#switchport trunk pruning vlan remove 3,10-15**

Manually Pruning VLANs

VTP to decide what VLANs would be allowed on a trunk and even went so far as to remove a VLAN from the prune eligible list.

SW1(config)**#interface FastEthernet 0/20**
SW1(config-if)**#switchport trunk allowed vlan remove 5**

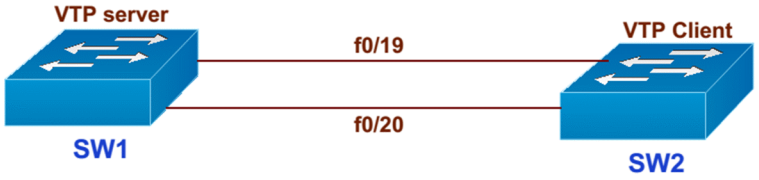
allows us to specify what VLAN or group of VLANs we want to be forwarded across a given trunk.

NOTE :
It is important that this command be applied on both ends of a given link.

```
sw-1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      999
Port        Vlans allowed on trunk
Fa0/20      1-1005
Port        Vlans allowed and active in management domain
Fa0/20      1
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      1
```

```
sw-1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      999
Port        Vlans allowed on trunk
Fa0/20      5
Port        Vlans allowed and active in management domain
Fa0/20      5
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      5
```

LAB: VTP Pruning:



TASK:

- Configure the link f0/19, f0/20 between SW1, SW2 as trunk links.
- SW1 = server , SW2 = Client
- domain : NOA (version2) password : noa123
- Create vlan 10,20,30,40 and VTP should sync with others.

```
SW1(config)#int range f0/19 - 20
SW1(config-if-range)#switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#exit

SW2(config)#int range f0/19  - 20
SW2(config-if-range)#switchport trunk encapsulation dot1q
SW2(config-if-range)#switchport mode trunk
SW2(config-if-range)#end

SW2#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/19      1-4094
Fa0/20      1-4094
Port        Vlans allowed and active in management domain
Fa0/19      1
Fa0/20      1
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/19      1
Fa0/20      1

SW1(config)#vtp domain NOA
SW1(config)#vtp password noa123
SW1(config)#vtp version 2
SW2(config)#  vtp mode Server

SW2(config)# vtp domain NOA
SW2(config)#  vtp password noa123
```

```
SW2(config)#  vtp version 2
SW2(config)#  vtp mode client

SW1(config)#vlan 10
SW1(config-vlan)#vlan 20
SW1(config-vlan)#vlan 30
SW1(config-vlan)#vlan 40
SW1(config-vlan)#exit
```

SW2#sh vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3
                                                 Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
40   VLAN0040                          active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

SW2#sh interfaces trunk

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/19      1-4094
Fa0/20      1-4094

Port        Vlans allowed and active in management domain
Fa0/19      1,10,20,30,40
Fa0/20      1,10,20,30,40

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/19      1,10,20,30,40
```

Fa0/20 1,10,20,30,40
SW2#

By default trunks allows all the vlan irrespective of whether they have active ports present on that vlan or not.

TASK:

- Configure VTP pruning on VTP server to ensure that the trunk links should prune the vlan which are not active on that particular switch;

SW1#sh vtp status
VTP Version : 2
Configuration Revision : 5
Maximum VLANs supported locally: 1005
Number of existing VLANs : 9
VTP Operating Mode : Server
VTP Domain Name : NOA
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0x34 0xFB 0xE4 0x98 0x79 0xEA 0x38 0x2C
Configuration last modified by 192.168.1.51 at 3-1-93 01:16:06
Local updater ID is 192.168.1.51 on interface Vl1 (lowest numbered VLAN interface found)

SW2#sh vtp status
VTP Version : 2
Configuration Revision : 5
Maximum VLANs supported locally : 1005
Number of existing VLANs : 9
VTP Operating Mode : Client
VTP Domain Name : NOA
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0x34 0xFB 0xE4 0x98 0x79 0xEA 0x38 0x2C
Configuration last modified by 192.168.1.51 at 3-1-93 01:16:06

SW1(config)#vtp pruning
Pruning switched on
SW1(config)#end

SW1#sh vtp status
VTP Version : 2
Configuration Revision : 6
Maximum VLANs supported locally : 1005
Number of existing VLANs : 9

VTP Operating Mode : Server
VTP Domain Name : NOA
VTP Pruning Mode : Enabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0x06 0xBC 0xF4 0x35 0xF9 0x8C 0x69 0xF7
Configuration last modified by 192.168.1.51 at 3-1-93 01:19:10
Local updater ID is 192.168.1.51 on interface Vl1 (lowest numbered VLAN interface found)

SW2#sh vtp status
VTP Version : 2
Configuration Revision : 6
Maximum VLANs supported locally : 1005
Number of existing VLANs : 9
VTP Operating Mode : Client
VTP Domain Name : NOA
VTP Pruning Mode : Enabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0x06 0xBC 0xF4 0x35 0xF9 0x8C 0x69 0xF7
Configuration last modified by 192.168.1.51 at 3-1-93 01:19:10

SW2#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/19	on	802.1q	trunking	1
Fa0/20	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/19	1-4094
Fa0/20	1-4094

Port	Vlans allowed and active in management domain
Fa0/19	1,10,20,30,40
Fa0/20	1,10,20,30,40

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/19	1
Fa0/20	1

- By default in my network i have only port f0/1 connected in vlan 1 and I have only vlan 1 active and it will not be pruned anyways by default.
- TO verify the pruning behavoiour i have vlan 10,20,30,40 created on server and synchronised on both switches

- create some svi interface for each vlan on both switches for verifying VTP pruning behaviour (in real networks we have PC connecting to their respective vlan, Here we are not adding any PC or routers for testing VTP pruning)

SW1#sh vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
40   VLAN0040                          active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

SW1(config)#int vlan 10
SW1(config-if)#exit
SW1(config)#int vlan 20
SW1(config-if)#exit

Once we create SVI for vvlan 10 and 20 on SW1 it will update the next switch about the ACtive vlan status and SW2 will add them in the not prune list.

SW2#sh interfaces trunk

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/19      1-4094
Fa0/20      1-4094

Port        Vlans allowed and active in management domain
Fa0/19      1,10,20,30,40
Fa0/20      1,10,20,30,40
```

```
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/19      1,10,20
Fa0/20      none
```

SW2#sh interfaces f0/19 pruning

```
Port        Vlans pruned for lack of request by neighbor
Fa0/19      30,40
Port        Vlan traffic requested of neighbor
Fa0/19      1,30,40
```

SW2(config)#int vlan 30
SW2(config-if)#int vlan 40
SW2(config-if)#end

Once we create SVI for vlan 30 and 40 on SW2 it will update the next switch about the ACtive vlan status and SW1 will add them in the not prune list.

SW1#sh interfaces trunk

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/19      1-4094
Fa0/20      1-4094

Port        Vlans allowed and active in management domain
Fa0/19      1,10,20,30,40
Fa0/20      1,10,20,30,40

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/19      1,30,40
Fa0/20      1
```

SW1#sh interfaces f0/19 pruning

```
Port        Vlans pruned for lack of request by neighbor
Fa0/19      10,20

Port        Vlan traffic requested of neighbor
Fa0/19      1,10,20
```

VTP Prune eligiblle List:

- If we want we can even add the vlan list which should not be pruned, as by default all the vlans are pruned except VLAN 1.

TASK:

- Create vlan 199 and ensure that vlan 199 should not get pruned even if they are not active ports.

Default vlan prune eligible list (2 -1001)

```
SW1(config)#vlan 199
SW1(config-vlan)#exit

SW1(config)#int range f0/19 - 20
SW1(config-if-range)#switchport trunk pruning vlan ?
  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  except  all VLANs except the following
  none    no VLANs
  remove  remove VLANs from the current list

SW1(config-if-range)#switchport trunk pruning vlan remove 199
SW1(config-if-range)#exit

SW2#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/19      1-4094
Fa0/20      1-4094

Port        Vlans allowed and active in management domain
Fa0/19      1,10,20,30,40,199
Fa0/20      1,10,20,30,40,199

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/19      1,10,20,199
Fa0/20      none

SW1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1
```

```
Port      Vlans allowed on trunk
Fa0/19    1-4094
Fa0/20    1-4094

Port      Vlans allowed and active in management domain
Fa0/19    1,10,20,30,40,199
Fa0/20    1,10,20,30,40,199

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/19    1,30,40,199
Fa0/20    1
```

TASK: Manual Pruning:

- Disable VTP pruning configured.
- Configure SW1/SW2 to allow only vlan 1,10,20,30,40 and vlan 199 on their respective trunk links (irespective whether they are active or not)

```
SW1(config)#no vtp pruning
Pruning switched off

SW1(config)#int range f0/19 -20
SW1(config-if-range)#switchport trunk allowed vlan 1,10,20,30,40,199
SW1(config-if-range)#exit


SW2(config)#int range f0/19 - 20
SW2(config-if-range)#switchport trunk allowed vlan 1,10,20,30,40,199
SW2(config-if-range)#end

SW2#sh interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/19    on        802.1q         trunking    1
Fa0/20    on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/19    1,10,20,30,40,199
Fa0/20    1,10,20,30,40,199

Port      Vlans allowed and active in management domain
Fa0/19    1,10,20,30,40,199
Fa0/20    1,10,20,30,40,199

Port      Vlans in spanning tree forwarding state and not pruned
```

```
Fa0/19      1,10,20,30,40,199
Fa0/20      10,20,30,40,199
```

TASK:

- Create vlan 50,60 and add them on the trunk list
- Configure Truk to remove vlan 10 from allowed vlan list.

```
SW1(config)#vlan 50
SW1(config-vlan)#vlan 60
SW1(config-vlan)#exit
```

SW1#sh vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
40   VLAN0040                          active
50   VLAN0050                          active
60   VLAN0060                          active
199  VLAN0199                          active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

SW1#sh interfaces trunk

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/19      1,10,20,30,40,199
Fa0/20      1,10,20,30,40,199

Port        Vlans allowed and active in management domain
Fa0/19      1,10,20,30,40,199
Fa0/20      1,10,20,30,40,199
```

```
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/19      1,10,20,30,40,199
Fa0/20      1
SW1(config)#int range f0/19 - 20
SW1(config-if-range)#switchport trunk allowed vlan add 50,60
SW1(config-if-range)#switchport trunk allowed vlan remove 10
SW1(config-if-range)#exit

SW1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/19      1,20,30,40,50,60,199
Fa0/20      1,20,30,40,50,60,199

Port        Vlans allowed and active in management domain
Fa0/19      1,20,30,40,50,60,199
Fa0/20      1,20,30,40,50,60,199

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/19      1,20,30,40,50,60,199
Fa0/20      1,50,60

SW2(config)#int range f0/19 - 20
SW2(config-if-range)#switchport trunk allowed vlan add 50,60
SW2(config-if-range)#switchport trunk allowed vlan remove 10
SW2(config-if-range)#end

SW2#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/19      1,20,30,40,50,60,199
Fa0/20      1,20,30,40,50,60,199

Port        Vlans allowed and active in management domain
Fa0/19      1,20,30,40,50,60,199
Fa0/20      1,20,30,40,50,60,199
```

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/19	1,20,30,40,50,60,199
Fa0/20	20,30,40,50,60,199

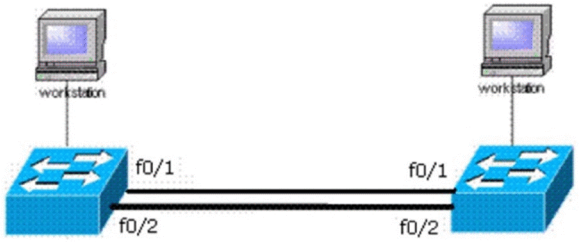
Spanning-tree protocol

Bridging loops

Redundant link between switches provides redundancy.

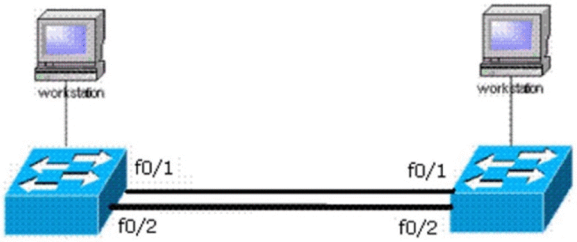
Also possibility to create loops when switches do broadcasts.

1. Broadcast storms
2. Mac-table instability
3. Multiple frame transmissions



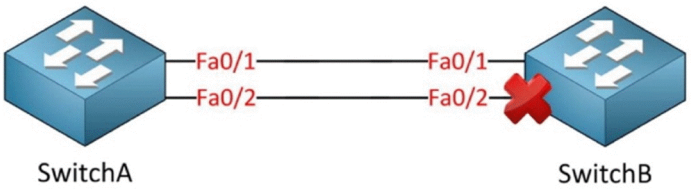
Bridging loops (solution)

1. Only one link between switches (no redundancy)
2. Shutdown extra link temporarily
   1. Manually (shutdown command)
   2. Automatically block extra links (done by STP)



Spanning-tree Protocol

- STP stop the loops which occurs when you have multiple links between switches
- STP stops avoiding Broadcast Storms, Multiple Frame Copies & Database instability.
- STP is a open standard (IEEE 802.1D)
- STP is enabled by default on all Cisco Catalyst switches

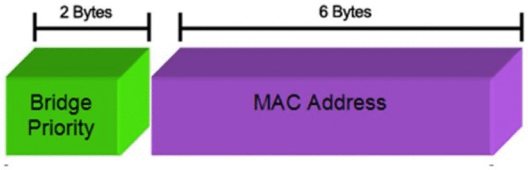


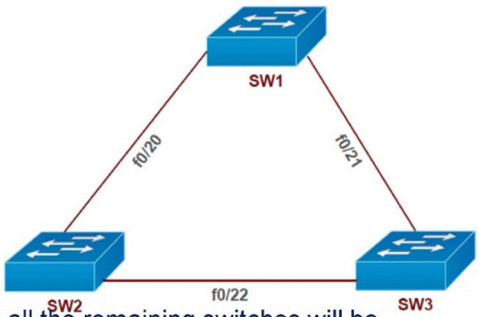
How STP works

1. Selecting the Root Bridge
2. Selecting the Root Port
3. Selecting Designated port & Non Designated port

1) Selecting the Root Bridge

- The bridge with the Best (Lowest) Bridge ID.
- Bridge ID = Priority + MAC address of the switch
- Out of all the switches in the network, one is elected as a root bridge that becomes the focal point in the network.



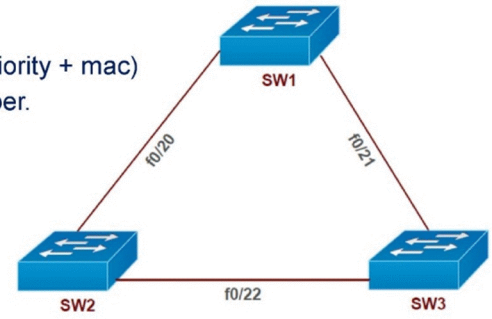


- Every LAN will have only one Root Bridge and all the remaining switches will be considered as Non-root Bridges.

2) Selecting the Root Port:

- Shortest path to the Root bridge
- Every Non-root Bridge looks the best way to go Root-bridge

1. least cost (Speed)
2. The Lowest forwarding Switch ID (priority + mac)
3. Lowest forwarding Physical Port Number.



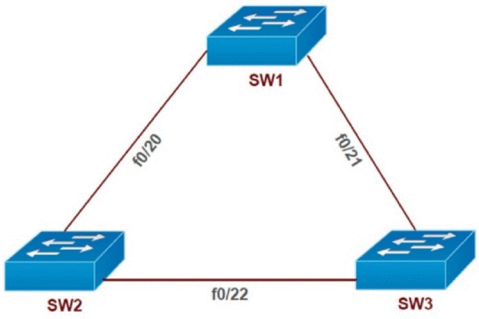
- For every non-root bridge there is only one root port.

STP Port Cost

Link Speed(Bandwidth)	Port Cost
10 mbps	100
100 bmps	19
1 gbps	4
10 gbps	2

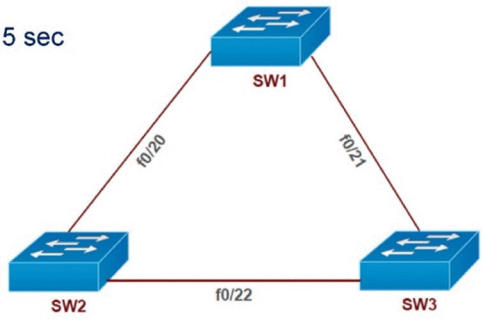
3) Selecting Designated port & Non Designated port

1. least cost (Speed)
2. least local Switch ID.
3. Lowest local Physical Port Number.



BPDU

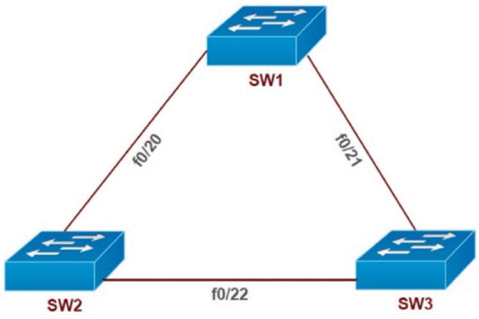
- All switches exchange information through what is called as Bridge Protocol Data Units (BPDUs)
- Hello = BPDUs are sent every 2 sec
- Max age(dead)= 20 sec
- Forward Delay (listening/learning time) = 15 sec



- A BPDU contains information regarding ports, switches, port priority and addresses.

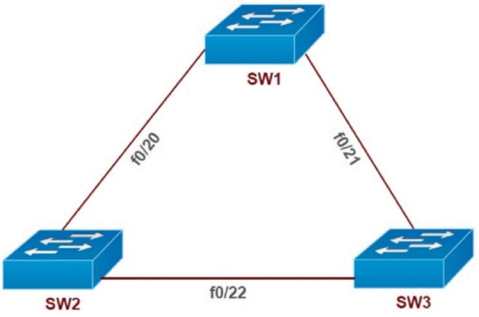
STP port states

- Blocking 20 Sec or No Limits.
- Listening 15 Sec.
- Learning 15 Sec.
- Forwarding No Limits.
- Disable No Limits.



Lab : verifying spanning-tree

Show Spanning-tree.
Show Spanning-tree vlan <no>
Show Spanning-tree root



Changing STP Timers

(Config)# Spanning-tree vlan <no> hello-time <>
(Config)# Spanning-tree vlan <no> forward-time <>
(Config)# Spanning-tree vlan <no> max-age <>

Hello

- time between each bridge protocol data unit (BPDU) that is sent on a port.
- 2 seconds (sec) by default, can tune the time to be between 1 and 10 sec.

forward delay

- Time that is spent in the listening and learning state.
- 15 sec by default, can tune the time to be between 4 and 30 sec.

max age

- The max age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information.
- 20 sec by default, can tune the time to be between 6 and 40 sec.

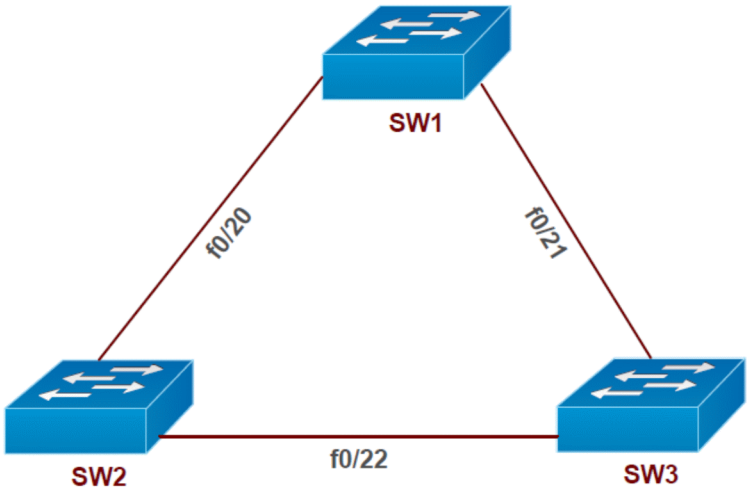
Chaning the port role

Modify the cost
- (Config-if)# Spanning-tree vlan <no> cost

Modify the bridge ID
- (Config-if)# Spanning-tree vlan <no> priority

Modify the port-priority
- (Config-if)# Spanning-tree vlan <no> port-priority

LAB: VERIFYING SPANNING-TREE



TASK: Find Root Bridge and alternate port (BLK)

```
Sw1#sh spanning-tree
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    32769
                     Address     0007.ECCD.AC82
                     Cost        19
                     Port        20(FastEthernet0/20)
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                     Address     00D0.580D.2EE0
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time  20

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/20           Root FWD 19        128.20   P2p
        Fa0/21           Desg FWD 19        128.21   P2p


SW2#sh spanning-tree
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    32769
                     Address     0007.ECCD.AC82
```

```
                This bridge is the root
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0007.ECCD.AC82
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/22           Desg FWD 19        128.22   P2p
```

```
SW3#sh spanning-tree
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID     Priority    32769
                      Address     0007.ECCD.AC82
                      Cost        19
                      Port        22(FastEthernet0/22)
                      Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                     Address     00D0.971E.4EAE
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time  20

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/21           Altn BLK 19        128.21   P2p
        Fa0/22           Root FWD 19        128.22   P2p
```

TASK:

- To verify the STP convergence process shutdown the SW1 f0/20 port and verify with Show spanning-tree

```
Sw1(config)#int f0/20
Sw1(config-if)#shutdown
```

Once f0/20 interface of SW1 or SW2 goes down, the alternate port f0/21 (SW3) comes to forwarding after delay of 50 sec

- BLK 20 sec
- LSN 15 sec
- LRN 15 sec

```
Sw1(config)#int f0/20
```

```
Sw1(config-if)#shutdown

SW3#sh spanning-tree
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    32769
                     Address     0007.ECCD.AC82
                     Cost        19
                     Port        22(FastEthernet0/22)
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                     Address     00D0.971E.4EAE
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time  20

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/21           Desg FWD 19        128.21   P2p
        Fa0/22           Root FWD 19        128.22   P2p
```

TASK: Configure F0/20 port of SW1 back to normal state (no shutdown)

```
        Sw1(config)# int f0/20
        Sw1(config-if)# no shutdown
        SW3#sh spanning-tree
              VLAN0001
                Spanning tree enabled protocol ieee
                Root ID    Priority    32769
                           Address     0007.ECCD.AC82
                           Cost        19
                           Port        22(FastEthernet0/22)
                           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

                Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                           Address     00D0.971E.4EAE
                           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                           Aging Time  20

              Interface        Role Sts Cost      Prio.Nbr Type
              ---------------- ---- --- --------- -------- --------------------------------
              Fa0/21           Altn BLK 19        128.21   P2p
              Fa0/22           Root FWD 19        128.22   P2p
```

```
Sw1#sh spanning-tree
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    32769
                     Address     0007.ECCD.AC82
                     Cost        19
                     Port        20(FastEthernet0/20)
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                     Address     00D0.580D.2EE0
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time  20

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/20           Root FWD 19        128.20   P2p
        Fa0/21           Desg FWD 19        128.21   P2p
```

- SW2 f0/21 goes back to BLK state
- SW1-/F0/20 comes back to normal forward state after 30 sec delay (15 sec LSN , 15 sec LRN)

TASK:

- Configure SW1 to be the Root Bridge for Vlan 1 by changing the Priority value
- Verify the STP port states changes once we change the Root bridge

Configuring Spanning Tree

To change the STP priority value, use the following:

Switch (config)# spanning-tree vlan <vlan_no> < priority value>

```
Sw1(config)#spanning-tree vlan 1 priority ?
  <0-61440>  bridge priority in increments of 4096

Sw1(config)#spanning-tree vlan 1 priority 0
Sw1(config)#end
Sw1#sh spanning-tree
    VLAN0001
      Spanning tree enabled protocol ieee
      Root ID    Priority    1
                 Address     00D0.580D.2EE0
                 This bridge is the root
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

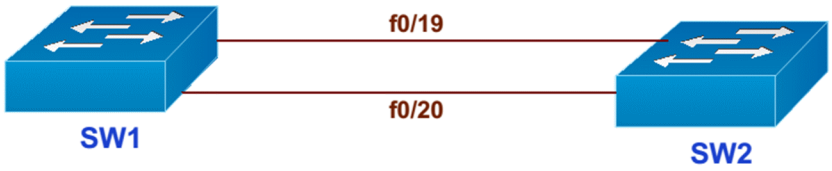
```
  Bridge ID  Priority    1  (priority 0 sys-id-ext 1)
             Address     00D0.580D.2EE0
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
```

```
SW3#sh spanning-tree
  VLAN0001
    Spanning tree enabled protocol ieee
    Root ID     Priority    1
                Address     00D0.580D.2EE0
                Cost        19
                Port        21(FastEthernet0/21)
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
               Address     00D0.971E.4EAE
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
               Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21           Root FWD 19        128.21   P2p
Fa0/22           Altn BLK 19        128.22   P2p
```

By default, STP is enabled for all active VLANs and on all ports of a switch. STP should remain enabled in a network to prevent bridging loops from forming.

- However, you might find that STP has been disabled in some way. If an entire instance of STP has been disabled, you can reenable it with the following global configuration command:
    - Switch(config)# spanning-tree vlan vlan-id
- If STP has been disabled for a specific VLAN on a specific port, you can reenable it with the following interface configuration command:
    - Switch (config-if)# spanning-tree vlan vlan-id

LAB: Tuning STP (cost/proirity/Timers)



TASK:

- Connect Sw1 and sw2 as per the digram on f0/19, f0/20 ports.
- Configure sw1 to be the root bridge for all vlans (also future vlan).
- Find what the rootports and Designated and blocking ports.

```
SW2#sh spanning-tree vlan 1
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    32769
                     Address     000b.be78.8300
                     This bridge is the root
                     Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                     Address     000b.be78.8300
                     Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time 300

          Interface        Role Sts Cost      Prio.Nbr Type
          ---------------- ---- --- --------- -------- --------------------------------
          Fa0/19           Desg FWD 19        128.19   P2p
          Fa0/20           Desg FWD 19        128.20   P2p
```

- By default in my case, sw2 is elected as Root Bridge based on best bridge ID.
- As per task we need to configure SW1 to become the Root Bridge with least prorirty value.

```
SW1#sh spanning-tree
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    32769
                     Address     000b.be78.8300
                     Cost        19
                     Port        19 (FastEthernet0/19)
                     Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
```

```
              Address     000b.bee2.fa00
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    Edge P2p
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/19           Root FWD 19        128.19   P2p
Fa0/20           Altn BLK 19        128.20   P2p
```

SW1 (config)#spanning-tree vlan 1-4094 root primary

SW1#sh spanning-tree vlan 1

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000b.bee2.fa00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     000b.bee2.fa00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    Edge P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        128.20   P2p
```

SW2#sh spanning-tree vlan 1

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000b.bee2.fa00
             Cost        19
             Port        19 (FastEthernet0/19)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000b.be78.8300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/19           Root FWD 19        128.19   P2p
Fa0/20           Altn BLK 19        128.20   P2p
```

- As per the default configurations sw2 f0/20 goes in to blocking state based on stp root port, and designtated port conditions.

TASK:

- Configure SW2 to ensure that f0/20 should be in forwarding state (f0/19 in to blocking)

```
SW2(config)#int f0/20
SW2(config-if)#spanning-tree cost 4
SW2(config-if)# end

or

SW2(config)#interface FastEthernet0/19
SW2(config-if)# spanning-tree cost 100
SW2(config-if)#exit

SW2#sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000b.bee2.fa00
             Cost        19
             Port        20 (FastEthernet0/20)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000b.be78.8300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/19           Altn BLK 100       128.19   P2p
Fa0/20           Root FWD 19        128.20   P2p
```

TASK

- Remove the cost configured in the previous task;
- Ensure that that you do the same cost by making changes other than SW2.(on sw1)

```
SW2(config)#int f0/19
SW2(config-if)#no spanning-tree cost 100
SW2(config-if)#exit

SW2#sh spanning-tree vlan 1
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    24577
                     Address     000b.bee2.fa00
                     Cost        19
                     Port        19 (FastEthernet0/19)
                     Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                     Address     000b.be78.8300
                     Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time 300

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/19           Root FWD 19        128.19   P2p
        Fa0/20           Altn BLK 19        128.20   P2p

SW1(config)#int f0/20
SW1(config-if)#spanning-tree port-priority ?
  <0-240>  port priority in increments of 16

SW1(config-if)#spanning-tree port-priority 0
SW1(config-if)#end

SW1#sh spanning-tree vlan 1
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    24577
                     Address     000b.bee2.fa00
                     This bridge is the root
                     Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
                     Address     000b.bee2.fa00
```

```
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    Edge P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        0.20     P2p
```

```
SW2#sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000b.bee2.fa00
             Cost        19
             Port        20 (FastEthernet0/20)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000b.be78.8300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/19           Altn BLK 19        128.19   P2p
Fa0/20           Root FWD 19        128.20   P2p
```

TASK: Changing STP timers

- Configure the root bridge so that switches generate Spanning-Tree hello packets every 3 seconds.
- When a new port becomes active, it should wait 20 seconds before transitioning to the forwarding state.
- If the switches do not hear a configuration message within 10 seconds, they should attempt reconfiguration.
- This configuration should affect all currently active VLANs and any additional VLANs created in the future.

```
SW1#sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000b.bee2.fa00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
```

```
        Address     000b.bee2.fa00
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    Edge P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19          0.20   P2p
```

Downstream devices from the root bridge inherit the timers configured on the root.

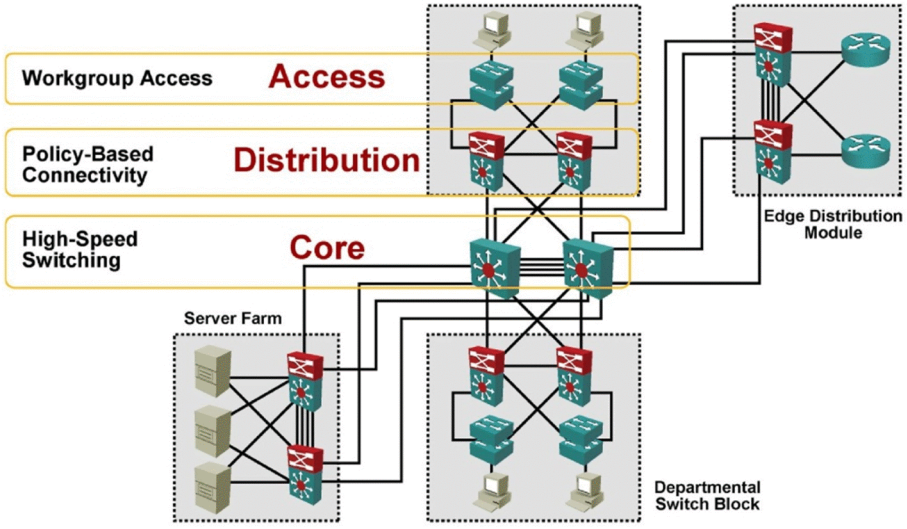
```
SW1(config)#spanning-tree vlan 1-4094 hello-time 3
SW1(config)#spanning-tree vlan 1-4094 forward-time 10
SW1(config)#spanning-tree vlan 1-4094 max-age 10
SW1(config)#end

SW1#sh spanning-tree vlan 1
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID     Priority    24577
                Address     000b.bee2.fa00
                This bridge is the root
                Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec

          Bridge ID Priority    24577 (priority 24576 sys-id-ext 1)
                Address     000b.bee2.fa00
                Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec
                Aging Time 300

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/1            Desg FWD 19        128.1    Edge P2p
        Fa0/19           Desg FWD 19        128.19   P2p
        Fa0/20           Desg FWD 19          0.20   P2p

SW2#sh spanning-tree vlan 1
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID     Priority    24577
                Address     000b.bee2.fa00
                Cost        19
                Port        20 (FastEthernet0/20)
                Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec
```

```
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000b.be78.8300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/19           Altn BLK 19        128.19   P2p
Fa0/20           Root FWD 19        128.20   P2p
```

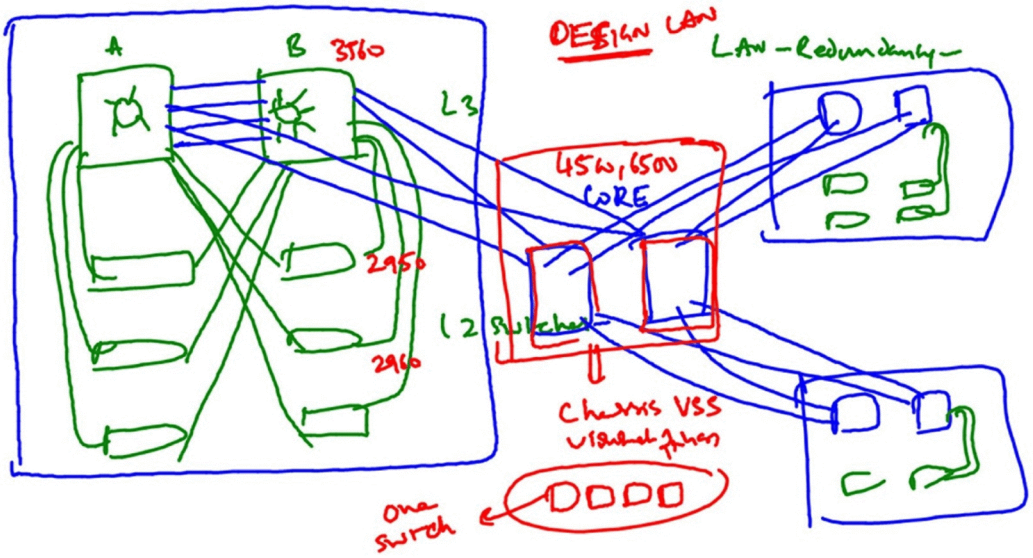
Optimizing STP

Selecting Root bridge, Portfast, Etherchannel , BPDU Guard/filter, Rootguard, loopguard, UDLD, errdisable

Hierarchical Campus Model

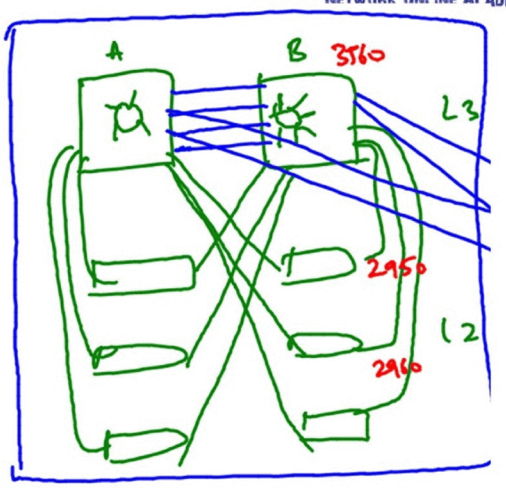


Hierarchical Campus Model



STP : Selecting Root Bridge

- Default root bridge election : **priority + Base Mac**
- Recommended to Select high speed Switch to be elected as Root Bridge .
  1. **Change priority**
  2. **Primary / Secondary**



STP : Selecting Root Bridge Configuration

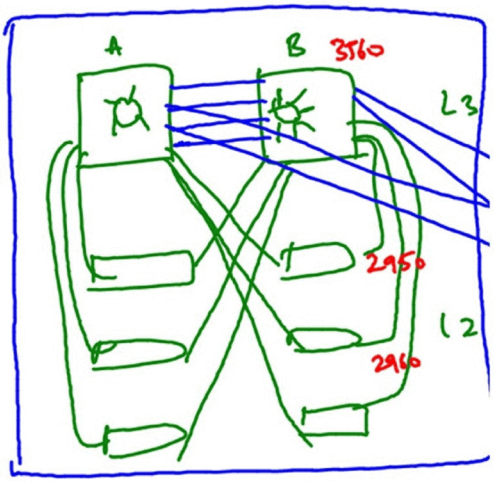
SW-A(config)#spanning-tree vlan 1 **root Primary**

SW-B(config)#spanning-tree vlan 1 **root Secondary**

OR

SW-A(config)#spanning-tree vlan 1 **priority 0**

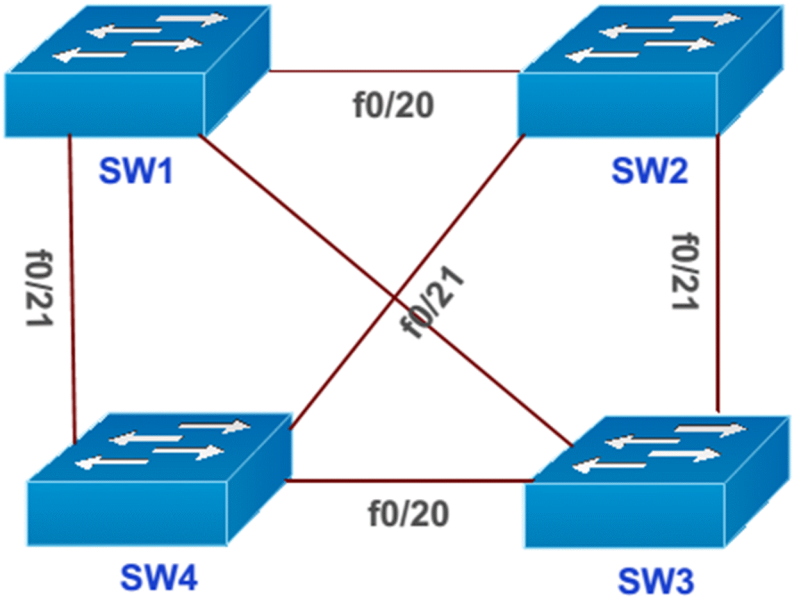
SW-B(config)#spanning-tree vlan 1 **priority 4096**



NOTE :

- Priority values can be only multiples of 4096
- Primary reduces priority by 8192 from default priority
- secondary reduces priority 4096 from default priority

LAB: Per VLAN STP:



TASK:

- Connect four switches as per the diagram.
- Find the Root bridge , root ports, alternate ports in the topology

SW1#sh spanning-tree

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0001.96C4.2C24
This bridge is the root.
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0001.96C4.2C24
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/20	Desg	FWD	19	128.20	P2p
Fa0/21	Desg	FWD	19	128.21	P2p
Fa0/22	Desg	FWD	19	128.22	P2p

SW2#sh spanning-tree
VLAN0001

```
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.96C4.2C24
             Cost        19
             Port        20(FastEthernet0/20)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.C994.B166
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Root FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
```

SW3#sh spanning-tree

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.96C4.2C24
             Cost        19
             Port        21(FastEthernet0/21)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.97DB.EE1C
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Altn BLK 19        128.20   P2p
Fa0/21           Root FWD 19        128.21   P2p
Fa0/22           Altn BLK 19        128.22   P2p
```

SW4#sh spanning-tree

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.96C4.2C24
             Cost        19
```

```
Port        22(FastEthernet0/22)
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
           Address     0005.5E81.6101
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Altn BLK 19        128.21   P2p
Fa0/22           Root FWD 19        128.22   P2p
```

- In this example, SW1 is the root Bridge and you can verify the root ports and alternate ports in the above outputs
- As per you topology it can vary as it based on Mac- address (vary from switch to switch)

TASK:

- Configure the links connecting between switches as Trunk links
- Configure VTP on all Four switches to synchronize the vlan information
- Create vlan 10,20,30,40 on SW1 and ensure that it sync with other switches.

ON SW1, SW2. SW3, SW4

```
SWx(config)#int range f0/20 - 22
SWx(config-if-range)#switchport trunk encapsulation dot1q
SWx(config-if-range)#switchport mode trunk

SWx(config)#vtp domain CCIE

SW1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
Fa0/21      on           802.1q         trunking      1
Fa0/22      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      1-1005
Fa0/21      1-1005
Fa0/22      1-1005

Port        Vlans allowed and active in management domain
Fa0/20      1
```

```
Fa0/21     1
Fa0/22     1

Port       Vlans in spanning tree forwarding state and not pruned
Fa0/20     1
Fa0/21     1
Fa0/22     1
```

SW2#sh int trunk

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
Fa0/21      on           802.1q         trunking      1
Fa0/22      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      1-1005
Fa0/21      1-1005
Fa0/22      1-1005

Port        Vlans allowed and active in management domain
Fa0/20      1
Fa0/21      1
Fa0/22      1
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      1
Fa0/21      1
Fa0/22      1
SW2#
```

SW3#sh interfaces trunk

```
Port        Mode         Encapsulation Status        Native vlan
Fa0/20      on           802.1q        trunking      1
Fa0/21      on           802.1q        trunking      1
Fa0/22      on           802.1q        trunking      1

Port        Vlans allowed on trunk
Fa0/20      1-1005
Fa0/21      1-1005
Fa0/22      1-1005

Port        Vlans allowed and active in management domain
Fa0/20      1
Fa0/21      1
Fa0/22      1
```

```
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      none
Fa0/21      1
Fa0/22      none
SW3#
```

```
SW4#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
Fa0/21      on           802.1q         trunking      1
Fa0/22      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      1-1005
Fa0/21      1-1005
Fa0/22      1-1005

Port        Vlans allowed and active in management domain
Fa0/20      1
Fa0/21      1
Fa0/22      1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      1
Fa0/21      none
Fa0/22      1
```



```
SW1(config)#vlan 10
SW1(config-vlan)#vlan 20
SW1(config-vlan)#vlan 30
SW1(config-vlan)#vlan 40
SW1(config-vlan)#exit
```

```
SW1#sh vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                          active
```

```
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

SW2#sh vlan brief

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```


SW3#sh vlan brief

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/23
                                                Fa0/24, Gig1/1, Gig1/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
```

```
1005 trnet-default                active
```

```
SW4#sh vlan brief
VLAN Name                         Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                            Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                            Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                            Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                            Fa0/17, Fa0/18, Fa0/19, Fa0/23
                                            Fa0/24, Gig1/1, Gig1/2
10   VLAN0010                     active
20   VLAN0020                     active
30   VLAN0030                     active
40   VLAN0040                     active
1002 fddi-default                 active
1003 token-ring-default           active
1004 fddinet-default              active
1005 trnet-default                active
```

TASK:

- Configure SW1 should be the Root Bridge for VLAN 10 .20 and Backup for VLAN 30,40
- Configure SW2 should be the Root Bridge for VLAN 30,40 and Backup for VLAN 10,20

Note:

- By default here SW1 will be the root bridge for all vlan as the priority value is same , and Sw1 is having the least MAC address of all (this may vary in your labs)

```
SW1#sh spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.96C4.2C24
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0001.96C4.2C24
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
```

```
Fa0/22          Desg FWD 19       128.22   P2p

SW1#sh spanning-tree vlan 20
  VLAN0020
    Spanning tree enabled protocol ieee
    Root ID    Priority    32788
               Address     0001.96C4.2C24
               This bridge is the root
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
               Address     0001.96C4.2C24
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
               Aging Time  20

  Interface        Role Sts Cost      Prio.Nbr Type
  ---------------- ---- --- --------- -------- --------------------------------
  Fa0/20           Desg FWD 19        128.20   P2p
  Fa0/21           Desg FWD 19        128.21   P2p
  Fa0/22           Desg FWD 19        128.22   P2p

SW1#sh spanning-tree vlan 30
  VLAN0030
    Spanning tree enabled protocol ieee
    Root ID    Priority    32798
               Address     0001.96C4.2C24
               This bridge is the root
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
               Address     0001.96C4.2C24
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
               Aging Time  20

  Interface        Role Sts Cost      Prio.Nbr Type
  ---------------- ---- --- --------- -------- --------------------------------
  Fa0/20           Desg FWD 19        128.20   P2p
  Fa0/21           Desg FWD 19        128.21   P2p
  Fa0/22           Desg FWD 19        128.22   P2p

SW1#sh spanning-tree vlan 40
  VLAN0040
    Spanning tree enabled protocol ieee
    Root ID    Priority    32808
```

```
        Address     0001.96C4.2C24
        This bridge is the root
        Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    32808  (priority 32768 sys-id-ext 40)
        Address     0001.96C4.2C24
        Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
```

You can configure a Catalyst switch to become the root bridge using one of two methods,

1. Manually setting the bridge priority value
   Switch(config)# spanning-tree vlan <vlan-list> priority <bridge-priority>

2. Causing the would-be root bridge switch to choose its own priority, based on some assumptions about other switches in the network using primary and secondary options. You can accomplish this with the following command:
   Switch(config)# spanning-tree vlan <vlan-id> root {primary | secondary}

- The bridge-priority value defaults to 32,768, but you can also assign a value of 0 to 65,535.
- If STP extended system ID is enabled (default is most switches) , the default bridge-priority is 32,768 plus the VLAN number.
- In that case, the value can range from 0 to 61,440, but only as multiples of 4096. A lower bridge priority is preferable.
- If the current root priority is less than that, the local switch sets its priority to 4096 less than the current root For the secondary root bridge, the root priority is set to an artificially low value of 28,672.

On SW1

```
SW1(config)#spanning-tree vlan 10,20 priority 0
SW1(config)#spanning-tree vlan 30,40 priority 4096
                    OR
SW1(config)#spanning-tree vlan 10,20 root primary
SW1(config)#spanning-tree vlan 30.40 root secondary
```

On SW2

```
SW2(config)#spanning-tree vlan 30,40 priority 0
SW2(config)#spanning-tree vlan 10,20 priority 4096
                    OR
```

```
SW2(config)#spanning-tree vlan  30,40 root primary
SW2(config)#spanning-tree vlan  10.20 root secondary


SW1#sh spanning-tree vlan 10
        VLAN0010
          Spanning tree enabled protocol ieee
          Root ID    Priority    10
                     Address     0001.96C4.2C24
                     This bridge is the root
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    10  (priority 0 sys-id-ext 10)
                     Address     0001.96C4.2C24
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time  20

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/20           Desg FWD 19        128.20   P2p
        Fa0/21           Desg FWD 19        128.21   P2p
        Fa0/22           Desg FWD 19        128.22   P2p

SW1#sh spanning-tree vlan 20
        VLAN0020
          Spanning tree enabled protocol ieee
          Root ID    Priority    20
                     Address     0001.96C4.2C24
                     This bridge is the root
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    20  (priority 0 sys-id-ext 20)
                     Address     0001.96C4.2C24
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time  20

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/20           Desg FWD 19        128.20   P2p
        Fa0/21           Desg FWD 19        128.21   P2p
        Fa0/22           Desg FWD 19        128.22   P2p

SW1#sh spanning-tree vlan 30
        VLAN0030
```

```
  Spanning tree enabled protocol ieee
  Root ID    Priority    30
             Address     0001.C994.B166
             Cost        19
             Port        20(FastEthernet0/20)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4126  (priority 4096 sys-id-ext 30)
             Address     0001.96C4.2C24
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Root FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
```

SW1#sh spanning-tree vlan 40

```
VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    40
             Address     0001.C994.B166
             Cost        19
             Port        20(FastEthernet0/20)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4136  (priority 4096 sys-id-ext 40)
             Address     0001.96C4.2C24
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Root FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
```

SW2#sh spanning-tree vlan 30

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    30
             Address     0001.C994.B166
             This bridge is the root
```

```
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

            Bridge ID  Priority    30  (priority 0 sys-id-ext 30)
                  Address     0001.C994.B166
                  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                  Aging Time  20

           Interface        Role Sts Cost      Prio.Nbr Type
           ---------------- ---- --- --------- -------- --------------------------------
           Fa0/20           Desg FWD 19        128.20   P2p
           Fa0/21           Desg FWD 19        128.21   P2p
           Fa0/22           Desg FWD 19        128.22   P2p
```

SW2#sh spanning-tree vlan 40

```
           VLAN0040
             Spanning tree enabled protocol ieee
             Root ID     Priority    40
                  Address     0001.C994.B166
                  This bridge is the root
                  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

             Bridge ID  Priority    40  (priority 0 sys-id-ext 40)
                  Address     0001.C994.B166
                  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                  Aging Time  20

           Interface        Role Sts Cost      Prio.Nbr Type
           ---------------- ---- --- --------- -------- --------------------------------
           Fa0/20           Desg FWD 19        128.20   P2p
           Fa0/21           Desg FWD 19        128.21   P2p
           Fa0/22           Desg FWD 19        128.22   P2p
```

SW2#sh spanning-tree vlan 10

```
           VLAN0010
             Spanning tree enabled protocol ieee
             Root ID     Priority    10
                  Address     0001.96C4.2C24
                  Cost        19
                  Port        20(FastEthernet0/20)
                  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

             Bridge ID  Priority    4106  (priority 4096 sys-id-ext 10)
                  Address     0001.C994.B166
                  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
              Aging Time  20

          Interface        Role Sts Cost      Prio.Nbr Type
          ---------------- ---- --- --------- -------- --------------------------------
          Fa0/20           Root FWD 19        128.20   P2p
          Fa0/21           Desg FWD 19        128.21   P2p
          Fa0/22           Desg FWD 19        128.22   P2p

SW2#sh spanning-tree vlan 20
          VLAN0020
            Spanning tree enabled protocol ieee
            Root ID     Priority    20
                    Address     0001.96C4.2C24
                    Cost        19
                    Port        20(FastEthernet0/20)
                    Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

            Bridge ID  Priority    4116  (priority 4096 sys-id-ext 20)
                    Address     0001.C994.B166
                    Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                    Aging Time  20

          Interface        Role Sts Cost      Prio.Nbr Type
          ---------------- ---- --- --------- -------- --------------------------------
          Fa0/20           Root FWD 19        128.20   P2p
          Fa0/21           Desg FWD 19        128.21   P2p
          Fa0/22           Desg FWD 19        128.22   P2p

SW3#sh spanning-tree vlan 10
          VLAN0010
            Spanning tree enabled protocol ieee
            Root ID     Priority    10
                    Address     0001.96C4.2C24
                    Cost        19
                    Port        21(FastEthernet0/21)
                    Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

            Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
                    Address     00D0.97DB.EE1C
                    Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                    Aging Time  20

          Interface        Role Sts Cost      Prio.Nbr Type
          ---------------- ---- --- --------- -------- --------------------------------
```

```
Fa0/20           Altn BLK 19       128.20   P2p
Fa0/21           Root FWD 19        128.21   P2p
Fa0/22           Altn BLK 19       128.22   P2p
```

SW3#sh spanning-tree vlan 20

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    20
             Address     0001.96C4.2C24
             Cost        19
             Port        21(FastEthernet0/21)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     00D0.97DB.EE1C
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Altn BLK 19       128.20   P2p
Fa0/21           Root FWD 19        128.21   P2p
Fa0/22           Altn BLK 19       128.22   P2p
```

SW3#sh spanning-tree vlan 30

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    30
             Address     0001.C994.B166
             Cost        19
             Port        22(FastEthernet0/22)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     00D0.97DB.EE1C
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Altn BLK 19       128.20   P2p
Fa0/21           Altn BLK 19       128.21   P2p
Fa0/22           Root FWD 19        128.22   P2p
```

SW3#sh spanning-tree vlan 40

VLAN0040

Spanning tree enabled protocol ieee

Root ID Priority 40

Address 0001.C994.B166

Cost 19

Port 22(FastEthernet0/22)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32808 (priority 32768 sys-id-ext 40)

Address 00D0.97DB.EE1C

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/20	Altn	BLK	19	128.20	P2p
Fa0/21	Altn	BLK	19	128.21	P2p
Fa0/22	Root	FWD	19	128.22	P2p

SW4#sh spanning-tree vlan 10

VLAN0010

Spanning tree enabled protocol ieee

Root ID Priority 10

Address 0001.96C4.2C24

Cost 19

Port 22(FastEthernet0/22)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)

Address 0005.5E81.6101

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/20	Desg	FWD	19	128.20	P2p
Fa0/21	Altn	BLK	19	128.21	P2p
Fa0/22	Root	FWD	19	128.22	P2p

SW4#sh spanning-tree vlan 20

VLAN0020

Spanning tree enabled protocol ieee

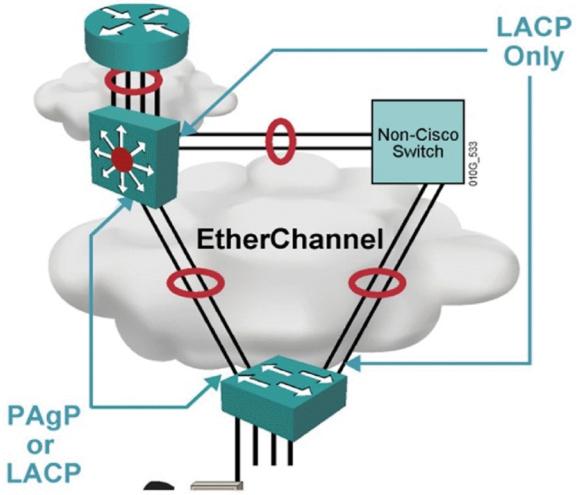
Root ID Priority 20

```
              Address     0001.96C4.2C24
              Cost        19
              Port        22(FastEthernet0/22)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0005.5E81.6101
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

          Interface        Role Sts Cost      Prio.Nbr Type
          ---------------- ---- --- --------- -------- --------------------------------
          Fa0/20           Desg FWD 19        128.20   P2p
          Fa0/21           Altn BLK 19        128.21   P2p
          Fa0/22           Root FWD 19        128.22   P2p

SW4#sh spanning-tree vlan 30
          VLAN0030
            Spanning tree enabled protocol ieee
            Root ID     Priority    30
                        Address     0001.C994.B166
                        Cost        19
                        Port        21(FastEthernet0/21)
                        Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

            Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
                        Address     0005.5E81.6101
                        Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                        Aging Time  20

          Interface        Role Sts Cost      Prio.Nbr Type
          ---------------- ---- --- --------- -------- --------------------------------
          Fa0/20           Desg FWD 19        128.20   P2p
          Fa0/21           Root FWD 19        128.21   P2p
          Fa0/22           Altn BLK 19        128.22   P2p

SW4#sh spanning-tree vlan 40
          VLAN0040
            Spanning tree enabled protocol ieee
            Root ID     Priority    40
                        Address     0001.C994.B166
                        Cost        19
                        Port        21(FastEthernet0/21)
                        Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    32808  (priority 32768 sys-id-ext 40)
             Address     0005.5E81.6101
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Root FWD 19        128.21   P2p
Fa0/22           Altn BLK 19        128.22   P2p
```

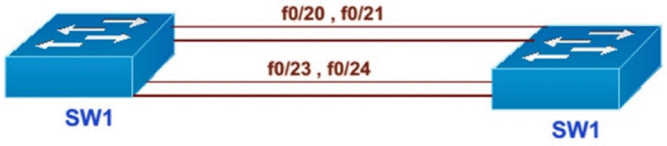
Etherchannel

- Used to aggregate bandwidth between multiple **L2/L3** interfaces.
- EtherChannel increases bandwidth and provides redundancy by aggregating individual links between switches.



Etherchannel (contd)

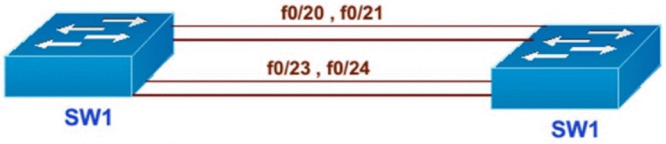
- EtherChannel load balances traffic over all the links in the bundle.
- Up to 8 links can be used to combine in to one logical link.
- Etherchannel can be configured as layer 2 or layer 3.
- Port-channel is the logical instance of the physical interfaces.



Etherchannel Modes:

EtherChannel can be dynamically configured between switches using two protocols.

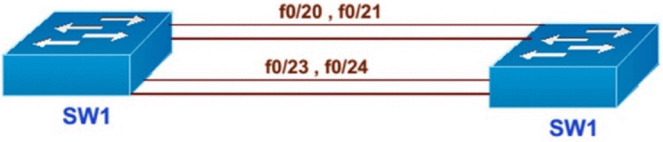
- -PAgP (Port Aggregation Protocol)
- -LACP (Link Aggregation Control Protocol)



Mode	Result
On	PAgP and LACP disabled (negotiation disable)
Auto	Passively listen for PAgP
Desirable	Actively negotiate PAgP
Passive	Passively listen for LACP
Active	Actively negotiate LACP

Successful combination of etherchannel would be:

On – On
Desirable – Desirable
Desirable – Auto
Active – Active
Active – Passive

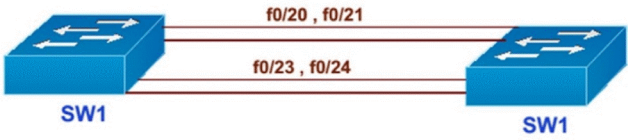


Switch(config)**#interface range f0/21 - 24**
Switch(config-if-range)**#channel-group 12 mode ?**
active Enable LACP unconditionally
auto Enable PAgP only if a PAgP device is detected
desirable Enable PAgP unconditionally
on Enable Etherchannel only
passive Enable LACP only if a LACP device is detected

Configuring EtherChannel Load Balancing

Switch(config)#**port-channel load-balance ?**

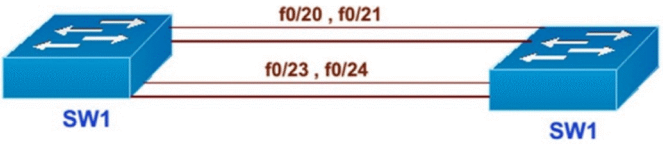
dst-ip	Dst IP Addr
dst-mac	Dst Mac Addr
src-dst-ip	Src XOR Dst IP Addr
src-dst-mac	Src XOR Dst Mac Addr
src-ip	Src IP Addr
src-mac	Src Mac Addr



dst-ip—Load distribution is based on the destination-host IP address.
dst-mac—Load distribution is based on the destination-host MAC address of the incoming packet.
src-dst-ip—Load distribution is based on the source-and-destination host-IP address.
src-dst-mac—Load distribution is based on the source-and-destination host-MAC address.
src-ip—Load distribution is based on the source-host IP address.
src-mac—Load distribution is based on the source-MAC address of the incoming packet.

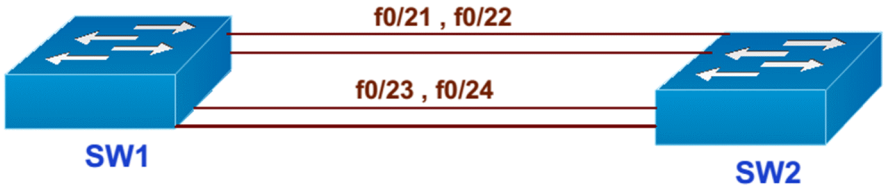
Some guidelines for EtherChannels

- Interfaces in the channel do not have to be physically next to each other or on the same module.
- All ports must be the same speed and duplex.
- All ports in the bundle should be enabled.
- None of the bundle ports can be a SPAN port.



- Assign an IP address to the logical Port Channel interface, not the physical ones, if using a Layer 3 EtherChannel.
- Put all bundle ports in the same VLAN, or make them all trunks.
- If they are trunks, they must all carry the same VLANs and use the same trunking mode.
- The configuration you apply to the Port Channel interface affects the entire EtherChannel.
- The configuration you apply to a physical interface affects only that interface.

LAB : Configruing Ether-Channel Using Pagp Protocol Negotiation



TASK

- Configure the Four links (f0/20 – 23) should appear as one logical link
- Ports should negotiate using Cisco Proprietary method.

SW1

```
SW1(config)#int range f0/20 - 23
SW1(config-if-range)#channel-protocol pagp
SW1(config-if-range)#channel-group 10 ?
        mode  Etherchannel Mode of the interface
SW1(config-if-range)#channel-group 10 mode ?
        active     Enable LACP unconditionally
        auto       Enable PAgP only if a PAgP device is detected
        desirable  Enable PAgP unconditionally
        on         Enable Etherchannel only
        passive    Enable LACP only if a LACP device is detected
SW1(config-if-range)#channel-group 10 mode desirable
```

SW2

```
SW2(config)#int range f0/20 - 23
SW2(config-if-range)#  channel-protocol pagp

SW2(config-if-range)#  channel-group 10 mode ?
        active     Enable LACP unconditionally
        auto       Enable PAgP only if a PAgP device is detected
        desirable  Enable PAgP unconditionally
        on         Enable Etherchannel only
        passive    Enable LACP only if a LACP device is detected
SW2(config-if-range)#  channel-group 10 mode auto
SW2(config-if-range)#exit

SW2#sh etherchannel summary
        Flags:  D - down        P - in port-channel
                I - stand-alone s - suspended
                H - Hot-standby (LACP only)
                R - Layer3      S - Layer2
                U - in use      f - failed to allocate aggregator
                u - unsuitable for bundling
```

```
        w - waiting to be aggregated
        d - default port

      Number of channel-groups in use: 1
      Number of aggregators:           1
      Group  Port-channel  Protocol    Ports
      ------+-------------+-----------+-----------------------------------------------
      10     Po10(SU)          PAgP    Fa0/20(P) Fa0/21(P) Fa0/22(P) Fa0/23(P)
```

SW2#sh spanning-tree

```
      VLAN0001
        Spanning tree enabled protocol ieee
        Root ID    Priority    32769
                   Address     0001.641A.B200
                   This bridge is the root
                   Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

        Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                   Address     0001.641A.B200
                   Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                   Aging Time  20

      Interface        Role Sts Cost      Prio.Nbr Type
      ---------------- ---- --- --------- -------- --------------------------------
      Po10             Desg LRN 7         128.27   Shr
```

SW2#sh ip int brief

```
      Interface              IP-Address      OK? Method Status                Protocol
      FastEthernet0/20       unassigned      YES unset  up                    up
      FastEthernet0/21       unassigned      YES unset  up                    up
      FastEthernet0/22       unassigned      YES unset  up                    up
      FastEthernet0/23       unassigned      YES unset  up                    up
      FastEthernet0/24       unassigned      YES unset  down                  down
      GigabitEthernet0/1     unassigned      YES unset  down                  down
      GigabitEthernet0/2     unassigned      YES unset  down                  down
      Vlan1                  unassigned      YES unset  administratively down down
      Port-channel 10        unassigned      YES unset  up                    up
```

SW1#sh spanning-tree

```
      VLAN0001
        Spanning tree enabled protocol ieee
        Root ID    Priority    32769
                   Address     0001.641A.B200
```

```
          Cost       7
          Port       27(Port-channel 10)
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
          Address     0060.4750.87A7
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po10             Root FWD 7         128.27   Shr
```

TASK: Configure the Portchannel 10 interface as Trunk link.

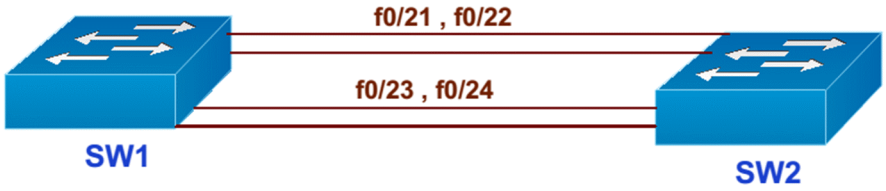
```
SW1(config)#  int port-channel 10
SW1(config-if)#  switchport trunk encapsulation dot1q
SW1(config-if)#  switchport mode trunk
SW1(config-if)#  exit


SW2(config)# int port-channel 10
SW2(config-if)#  switchport trunk encapsulation dot1q
SW2(config-if)#  switchport mode trunk
SW2(config-if)#  exit

SW2#sh interfaces trunk
          Port        Mode         Encapsulation  Status        Native vlan
          Fa0/20      on           802.1q         trunking      1
          Fa0/21      on           802.1q         trunking      1
          Fa0/22      on           802.1q         trunking      1
          Fa0/23      on           802.1q         trunking      1
          Po10        on           802.1q         trunking      1
          Port        Vlans allowed on trunk
          Fa0/20      1-1005
          Fa0/21      1-1005
          Fa0/22      1-1005
          Fa0/23      1-1005
          Po10        1-1005
          Port        Vlans allowed and active in management domain
          Fa0/20      1
          Fa0/21      1
          Fa0/22      1
          Fa0/23      1
          Po10        1
```

```
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      none
Fa0/21      none
Fa0/22      none
Fa0/23      none
Po10        none
```

- Any changes applied on the port channel automatically effect on all the physical interfaces
- Port channel will work as long as at least one interface in the group is up and running

```
SW2#sh etherchannel summary
        Flags:  D - down        P - in port-channel
                I - stand-alone s - suspended
                H - Hot-standby (LACP only)
                R - Layer3      S - Layer2
                U - in use      f - failed to allocate aggregator
                u - unsuitable for bundling
                w - waiting to be aggregated
                d - default port
        Number of channel-groups in use: 1
        Number of aggregators:           1

        Group  Port-channel  Protocol    Ports
        ------+-------------+-----------+-----------------------------------------------
        10     Po10(SU)          PAgP    Fa0/20(P) Fa0/21(P) Fa0/22(P) Fa0/23(P)
```

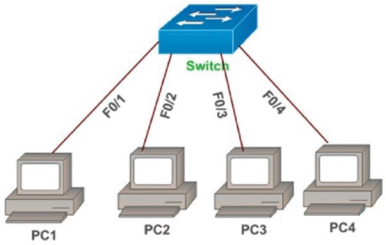
Layer 3 Etherchannel



- In order to configure layer 3 port channel interface, the member ports must be configured with no switchport command before using port-channel commands.
- If the channel-group command is issued before the no switchport command on the physical interfaces, the logical port-channel interface will be created as the default of Layer 2, and this cannot be changed afterward.
- To fix this problem, simply issue the no switchport command before the channelgroup command.
- If configured properly, the state of the port-channel from the show etherchannel summary command should show RU for routed and in use.

Spanning tree Portfast

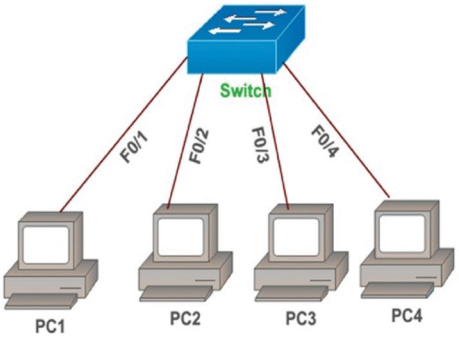
- Cisco-proprietary enhancement to Spanning Tree.
- helps speed up network convergence on access ports.
- Port Fast causes a port to enter the spanning-tree forwarding state immediately, bypassing the listening and learning states.



NOTE :

- PortFast should be used only when connecting a single end station to a switch port.
- If you enable PortFast on a port connected to another networking device, such as a switch, you can create network loops.

Portfast Configuration



Portfast on specific ports

(config)# interface range f0/1 - 10

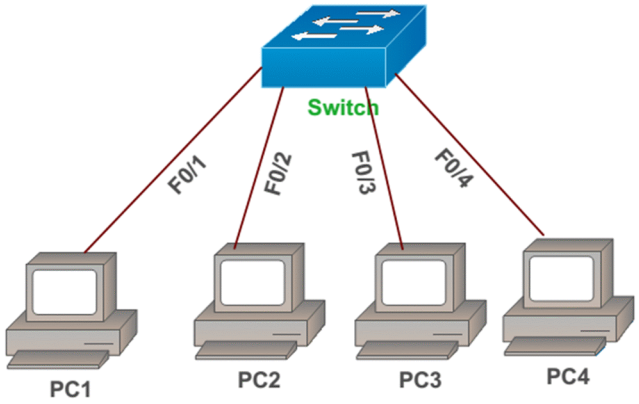
(config-if) spanning-tree portfast

OR

Portfast on all access ports globally using one command

(config)#spanning-tree portfast default

LAB: STP PORT FAST:



TASK:

- Connect Four PC in the LAN as per the Diagram.
- Shutdown the ports on Switch & reconfigure No shutdown and observer the ports going through LSN & LRN stages of STP process before they come to FWD…

```
Switch(config)#int range f0/1 - 4
Switch(config-if-range)#  shutdown
Switch(config-if-range)#  no shutdown

 Switch#sh spanning-tree

        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    32769
                     Address     0001.6336.1BA3
                     This bridge is the root
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                     Address     0001.6336.1BA3
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time  20

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/1            Desg LSN 19        128.1    P2p
        Fa0/2            Desg LSN 19        128.2    P2p
        Fa0/4            Desg LSN 19        128.4    P2p
        Fa0/3            Desg LSN 19        128.3    P2p

Switch#sh spanning-tree
        VLAN0001
          Spanning tree enabled protocol ieee
```

```
  Root ID    Priority    32769
             Address     0001.6336.1BA3
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.6336.1BA3
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg LRN 19        128.1    P2p
Fa0/2            Desg LRN 19        128.2    P2p
Fa0/4            Desg LRN 19        128.4    P2p
Fa0/3            Desg LRN 19        128.3    P2p
```

```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.6336.1BA3
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.6336.1BA3
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

- All the ports connecting to end devices go through listening and Learning states by default before they comes to Forwarding State
- This is the default STP Loop prevention mechanism on switches
- Here we want these access ports to bypass the LSN, LRN stages and transition to FWD immediately
- To do this we configure portfast on these ports (used only on access ports)

```
Switch(config)#int range f0/1 - 4
```

```
Switch(config-if-range)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 4 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.

Switch(config-if-range)#end
```

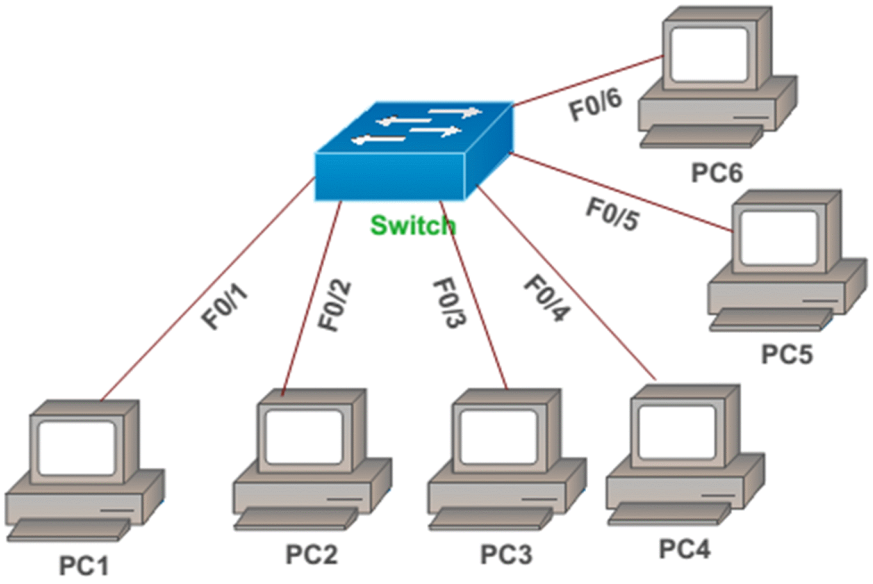
TO verify:

```
Switch(config)#interface range f0/1 - 4
Switch(config-if-range)#shutdown
Switch(config-if-range)#no shutdown

Switch#sh spanning-tree
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    32769
                     Address     0001.6336.1BA3
                     This bridge is the root
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                     Address     0001.6336.1BA3
                     Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                     Aging Time  20

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/1            Desg FWD 19        128.1    P2p
        Fa0/2            Desg FWD 19        128.2    P2p
        Fa0/4            Desg FWD 19        128.4    P2p
        Fa0/3            Desg FWD 19        128.3    P2p
```

Once port fast configured on the interfaces all the ports transitions to Forwarding immediately without LSN, LRN states

TASK:

- Configure Switch to ensure that all future access ports should bypass LSN, LRN states using single command.



Switch(config)#spanning-tree portfast default
Switch(config)#end

To Verity Connect some end devices on portf0/5 – 6 to verify

Switch#sh spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0001.6336.1BA3
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0001.6336.1BA3
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/6	Desg	FWD	19	128.6	P2p
Fa0/5	Desg	FWD	19	128.5	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.3	P2p

BPDU Guard

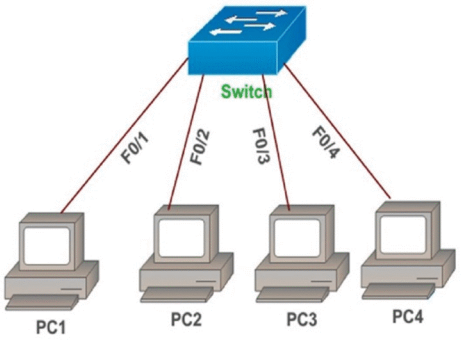
- BPDU Guard prevents loops if another switch is attached to a Portfast port.
- When BPDU Guard is enabled on an inter-face, it is put into an error-disabled state (basically, shut down) if a BPDU is received on the interface.
- It can be enabled at either global config mode affects all (Portfast interfaces) or at interface mode.
- Portfast does not need to be enabled for it to be configured at a specific interface.

(config)# spanning-tree portfast bpduguard default

OR

(config-if)# spanning-tree bpduguard enable

 # show spanning-tree summary totals



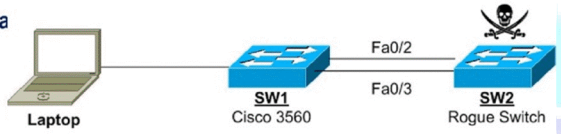
BPDU Guard verification

SW1(config)**#spanning-tree portfast bpduguard defa**

Or

SW1(config)**# interface f0/2**

SW1(config-if)**#spanning-tree bpduguard enable**



%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/2 with BPDU Guard enabled. Disabling port.

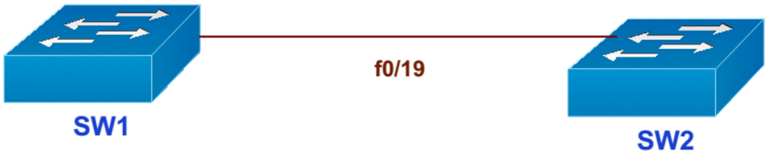
%PM-4-ERR_DISABLE: bpduguard error detected on Fa0/2, putting Fa0/2 in err-disable state

SW1**#show interface status err-disabled**

Port Name	Status	Reason Err-disabled Vlans
Fa0/2	err-disabled	bpduguard

The port is err-disabled and, unless err-disabled recovery is enabled, has to be manually re-enabled via shut/no shut.

LAB: BPDU Guard:



TASK:

- Connect link between SW1 and SW2 f0/19 and shutdown all remaining ports.
- Configure SW2 f0/19 as layer 3 ports to test BPDU guard feature.
- Enable BPDU Gaurd and portfast feature on SW1.

```
SW2(config)#int f0/19
SW2(config-if)#no switchport
SW2(config-if)#ip address 10.0.0.1 255.0.0.0
SW2(config-if)#exit

SW1(config)#vlan 10
SW1(config-vlan)#exit

SW1(config)#int f0/19
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#spanning-tree portfast
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#exit

SW1#show spanning-tree interface f0/19 detail
 Port 19 (FastEthernet0/19) of VLAN0010 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.19.
   Designated root has priority 32778, address 000b.bee2.fa00
   Designated bridge has priority 32778, address 000b.bee2.fa00
   Designated port id is 128.19, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 58, received 0
```

TASK: Reconfigure F0/19 port on sw2 back to layer 2 port (adding switchport)

```
SW2(config)#int f0/19
SW2(config-if)#switchport
SW2(config-if)#exit
```

```
SW1#sh interfaces f0/19 status err-disabled
Port      Name               Status       Reason
Fa0/19                       err-disabled bpduguard

SW1#sh interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          a-full  a-100 10/100BaseTX
Fa0/19                       err-disabled 10         auto    auto 10/100BaseTX
```

TASK: Configure f0/19 port back to layer 3 port and ensure that port comes back up..

```
SW2(config-if)#int f0/19
SW2(config-if)#no switchport
SW2(config-if)#ip address 10.0.0.1 255.0.0.0
SW2(config-if)#exit

SW2(config)#do sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/19       10.0.0.1        YES manual down                  down

SW2(config)#int f0/19
SW2(config-if)#shutdown
SW2(config-if)#no shutdown
SW2(config-if)#end

SW2#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/19       10.0.0.1        YES manual up                    up

SW2#sh interfaces status
Fa0/19                       connected    routed     a-full  a-100 10/100BaseTX
```

TASK:

- Configure Err-disable recovery for BPDU GAURD such that port should come up automatcially after 60 sec of err-disable state.

```
SW1(config)#errdisable recovery cause bpduguard
SW1(config)#errdisable recovery interval ?
  <30-86400>  timer-interval(sec)

SW1(config)#errdisable recovery interval 60
SW1(config)#exit

SW1#sh errdisable recovery
```

```
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Enabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled
loopback             Disabled

Timer interval: 60 seconds
Interfaces that will be enabled at the next timeout:
```

TASK: Test by chaning layer 3 inteface f0/19 to switchport and then back to layer 3 ;

```
SW2(config)#int f0/19
SW2(config-if)#switchport
SW2(config-if)#exit

SW1#sh interfaces f0/19 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/19                       err-disabled 10         auto    auto 10/100BaseTX

SW2(config)#int f0/19
SW2(config-if)#no switchport
SW2(config-if)#ip address 10.0.0.1 255.0.0.0
SW2(config-if)#end

SW1#sh errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Enabled
security-violatio    Disabled
channel-misconfig    Disabled
```

```
vmps                Disabled
pagp-flap           Disabled
dtp-flap            Disabled
link-flap           Disabled
l2ptguard           Disabled
psecure-violation   Disabled
gbic-invalid        Disabled
dhcp-rate-limit     Disabled
unicast-flood       Disabled
storm-control       Disabled
arp-inspection      Disabled
loopback            Disabled

Timer interval: 60 seconds
Interfaces that will be enabled at the next timeout:
Interface   Errdisable reason   Time left(sec)
---------   -----------------   --------------
Fa0/19      bpduguard           25
```

SW1#sh errdisable recovery

```
ErrDisable Reason   Timer Status
-----------------   --------------
udld                Disabled
bpduguard           Enabled
security-violatio   Disabled
channel-misconfig   Disabled
vmps                Disabled
pagp-flap           Disabled
dtp-flap            Disabled
link-flap           Disabled
l2ptguard           Disabled
psecure-violation   Disabled
gbic-invalid        Disabled
dhcp-rate-limit     Disabled
unicast-flood       Disabled
storm-control       Disabled
arp-inspection      Disabled
loopback            Disabled

Timer interval: 60 seconds
Interfaces that will be enabled at the next timeout:
Interface   Errdisable reason   Time left(sec)
---------   -----------------   --------------
Fa0/19      bpduguard           7
```

```
SW1#sh interfaces f0/19 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/19                       connected    10         a-full  a-100 10/100BaseTX
```

TASK:

- Reconfigure and verify the same task by removing on interface mode and enabling BPDU guard on global configuration mode:

```
SW1(config)#int f0/19
SW1(config-if)#no spanning-tree portfast
SW1(config-if)#no  spanning-tree bpduguard enable
SW1(config-if)#exit

SW1(config)#no errdisable recovery cause bpduguard
SW1(config)#no errdisable recovery interval 60

SW1#sh errdisable recovery
    ErrDisable Reason    Timer Status
    -----------------    --------------
    udld                 Disabled
    bpduguard            Disabled
    security-violatio    Disabled
    channel-misconfig    Disabled
    vmps                 Disabled
    pagp-flap            Disabled
    dtp-flap             Disabled
    link-flap            Disabled
    l2ptguard            Disabled
    psecure-violation    Disabled
    gbic-invalid         Disabled
    dhcp-rate-limit      Disabled
    unicast-flood        Disabled
    storm-control        Disabled
    arp-inspection       Disabled
    loopback             Disabled

    Timer interval: 300 seconds
    Interfaces that will be enabled at the next timeout:

SW1#sh interfaces f0/19 status
    Port      Name               Status       Vlan       Duplex  Speed Type
    Fa0/19                       connected    10         a-full  a-100 10/100BaseTX
```

```
SW1(config)#spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.

SW1(config)#spanning-tree portfast bpduguard default

SW1(config)#errdisable recovery cause bpduguard
SW1(config)#errdisable recovery interval 60

SW2(config)#int f0/19
SW2(config-if)#switchport
SW2(config-if)#exit

SW2#sh interfaces f0/19 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/19                       notconnect   1            auto   auto 10/100BaseTX


SW1#sh interfaces f0/19 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/19                       err-disabled 10           auto   auto 10/100BaseTX

SW2(config)#int f0/19
SW2(config-if)#no switchport
SW2(config-if)#ip address 10.0.0.1 255.0.0.0
SW2(config-if)#end

SW1#sh errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Enabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
```

```
storm-control       Disabled
arp-inspection      Disabled
loopback            Disabled

Timer interval: 60 seconds
Interfaces that will be enabled at the next timeout:
Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Fa0/19       bpduguard                 3
```

SW1#sh interfaces f0/19 status

```
Port      Name               Status       Vlan       Duplex Speed Type
Fa0/19                       connected    10         a-full  a-100 10/100BaseTX
```

BPDU Filtering

(config)# **spanning-tree portfast bpdufilter default**

- If a Portfast interface receives any BPDUs, it is taken out of Portfast status.
- The interfaces still send some BPDUs at the link-up,
- if a BPDU is received, the interface loses its Port Fast status and BPDU Filtering is disabled.

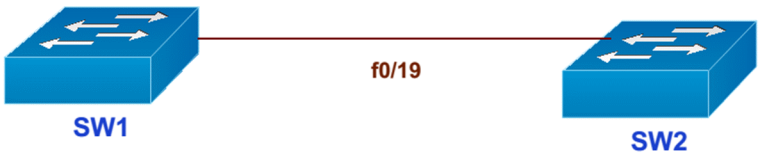
(config-if)# **spanning-tree bpdufilter enable**

- The interface doesn't send any BPDU and ignores the received ones.
- The port is not shutdown and this basically **disables spanning-tree on the interface.**

LAB: BPDU filter (interface level)

BPDU Filter is used to terminate the STP domain, but it has a different functionality: it can also be configured globally or at the interface level. However, behavior is different based on this; this was not the case For BPDU Guard, this had the same functionality regardless of how it was enabled.

When configured at the interface level, BPDU Filter silently drops all received inbound BPDUs and does not send any outbound BPDUs on the port. There is no violation option for BPDU Filter, so the port never goes into err-disabled state. BPDU Filter needs to be carefully enabled at the port level, because it will cause permanent loops if on the other end of the link a switch is connected and the network is physically looped; in this case, STP will not be able to detect the loop and the network will become unusable within seconds.



TASK:

- Connect link between SW1 and SW2 f0/19 and shutdown all remaining ports.
- Configure sw2 f0/19 as layer 3 ports to test BPDU guard feature.
- Enable BPDU Gaurd and portfast feature on sw1.

```
SW2(config)#int f0/19
SW2(config-if)#no switchport
SW2(config-if)#ip address 10.0.0.1 255.0.0.0
SW2(config-if)#exit

SW1(config)#vlan 10
SW1(config-vlan)#exit

SW1(config)#int f0/19
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#spanning-tree portfast
SW1(config-if)#spanning-tree bpdufilter enable
SW1(config-if)#exit

SW1#sh spanning-tree interface f0/19 detail
      Port 19 (FastEthernet0/19) of VLAN0010 is forwarding
        Port path cost 19, Port priority 128, Port Identifier 128.19.
        Designated root has priority 32778, address 000b.bee2.fa00
        Designated bridge has priority 32778, address 000b.bee2.fa00
        Designated port id is 128.19, designated path cost 0
        Timers: message age 0, forward delay 0, hold 0
```

Number of transitions to forwarding state: 1
Link type is point-to-point by default
Bpdu filter is enabled
BPDU: sent 9, received 0

TASK: Configure SW2 f0/19 as layer 2 ports so that it can start sending BPDU

SW2(config)#int f0/19
SW2(config-if)#switchport
SW2(config-if)#end
SW2#

SW1#sh interfaces f0/19 status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/19		connected	10	a-full	a-100	10/100BaseTX

SW1#sh spanning-tree int f0/19 detail

Port 19 (FastEthernet0/19) of VLAN0010 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.19.
Designated root has priority 32778, address 000b.bee2.fa00
Designated bridge has priority 32778, address 000b.bee2.fa00
Designated port id is 128.19, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
Bpdu filter is enabled
BPDU: sent 0, received 33

SW1#sh interfaces f0/19 status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/19		connected	10	a-full	a-100	10/100BaseTX

SW1#sh spanning-tree vlan 10

VLAN0010
Spanning tree enabled protocol ieee
Root ID Priority 32778
Address 000b.bee2.fa00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 000b.bee2.fa00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/19           Desg FWD 19        128.19   P2p
```

TASK: BPDU global configuration mode:

- Remove the Bpdu filter on the interface and enable it globally.
- Configure portfast on f0/19 on Sw1 for verification.

```
SW2(config)#  int f0/19
SW2(config-if)#  no switchport
SW2(config-if)#  ip address 10.0.0.1 255.0.0.0
SW2(config-if)#end

SW1(config)#int f0/19
SW1(config-if)#spanning-tree portfast
SW1(config-if)#no  spanning-tree bpdufilter enable
SW1(config-if)#exit

SW1(config)#spanning-tree portfast bpdufilter default
SW1(config)#end

SW1#sh interfaces f0/19 status
  Port      Name               Status       Vlan       Duplex  Speed Type
  Fa0/19                       connected    10         a-full  a-100 10/100BaseTX

SW1#sh spanning-tree vlan 10
  VLAN0010
    Spanning tree enabled protocol ieee
    Root ID     Priority    32778
                Address     000b.bee2.fa00
                This bridge is the root
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
                Address     000b.bee2.fa00
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time 300

  Interface        Role Sts Cost      Prio.Nbr Type
  ---------------- ---- --- --------- -------- --------------------------------
  Fa0/19           Desg FWD 19        128.19   Edge P2p

SW1#sh spanning-tree int f0/19 detail
```

Port 19 (FastEthernet0/19) of VLAN0010 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.19.
Designated root has priority 32778, address 000b.bee2.fa00
Designated bridge has priority 32778, address 000b.bee2.fa00
Designated port id is 128.19, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
The port is in the portfast mode
Link type is point-to-point by default
Bpdu filter is enabled by default
BPDU: sent 11, received 0

SW2(config-if)#int f0/19
SW2(config-if)#switchport
SW2(config-if)#end

SW1#sh spanning-tree int f0/19 detail
Port 19 (FastEthernet0/19) of VLAN0010 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.19.
Designated root has priority 32769, address 000b.be78.8300
Designated bridge has priority 32769, address 000b.be78.8300
Designated port id is 128.19, designated path cost 0
Timers: message age 2, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 0, received 4

SW1#show spanning-tree interface fastEthernet0/19 portfast
VLAN0010 disabled

SW2(config)#int f0/19
SW2(config-if)#no switchport

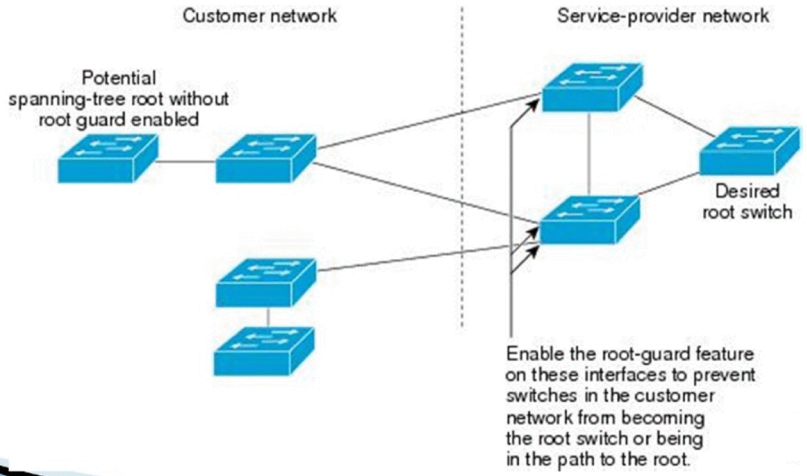
SW1#show spanning-tree interface fastEthernet0/19 portfast
VLAN0010 enabled

SW1#sh spanning-tree int f0/19 detail
Port 19 (FastEthernet0/19) of VLAN0010 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.19.
Designated root has priority 32778, address 000b.bee2.fa00
Designated bridge has priority 32778, address 000b.bee2.fa00
Designated port id is 128.19, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1

The port is in the portfast mode
Link type is point-to-point by default
Bpdu filter is enabled by default
BPDU: sent 11, received 0

Root Guard

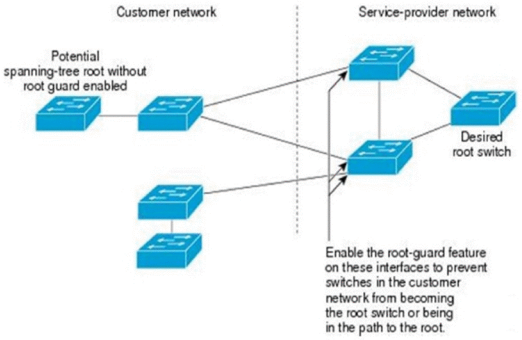
- prevents the wrong switch from becoming the Spanning Tree root.
- If a Root Guard port receives a superior BPDU that might cause it to become a root port, the port is put into "root-inconsistent" state and does not pass traffic through it.
- If the port stops receiving these BPDUs, it automatically re-enables itself.



Configuring Rootport

(config)# interface f0/19
(config-if)# spanning-tree guard root

Ports disabled by root guard can be viewed with **#**
show spanning-tree inconsistentports

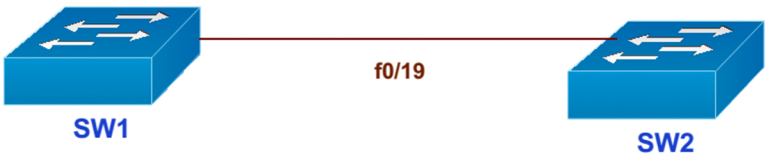


NOTE ;

- Enabled on ports other than the root port and on switches other than the root.
- "root guard" command cannot be used on root switch (because this command is based on blocked port – while a root switch can't have a blocked port

LAB : ROOT GUARD

- Root Guard is similar to the BPDU Guard feature in the manner in which it is used to detect STP packets and disable the interface they were received on.
- The difference between them is that with Root Guard, the interface is only logically disabled (via Root Inconsistentstate) if a superior BPDU is received on the port with Root Guard enabled.
- Root Inconsistentstate is similar to blocking state, in that BPDUs are not sent outbound but accepted inbound, and of course all received frames are dropped.
- The switch automatically recovers the port from Root Inconsistentand starts negotiating the new port state and role, as soon as superior BPDUs are no longer received inbound.
- A superior BPDU indicates a better cost to the root bridge than what is currently installed.
- Therefore, in terms of design, this feature is used to prevent a rogue device from announcing itself as the new root bridge and possibly implementing a layer 2 man-in-the-middle attack. Root Guard can be enabled only at the port level and basically prevents a Designated port from becoming Non-Designated.
- You will want to configure this functionality on the Root Bridge itself.
- Verify that Root Guard is enabled for all VLANs, for example on FastEthernet0/19 port.



TASK:

- Configure SW1 so that STP logically blocks Ethernet links connected to SW2 if any of port on SW2 tries to become Root Bridge for any VLAN.

```
SW1#sh spanning-tree vlan 1
    VLAN0001
      Spanning tree enabled protocol ieee
      Root ID    Priority    32769
                 Address     000b.be78.8300
                 Cost        19
                 Port        19 (FastEthernet0/19)
                 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                 Address     000b.bee2.fa00
                 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                 Aging Time 15

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/1            Desg FWD 19        128.1    Edge P2p
```

```
Fa0/19          Root FWD 19        128.19   P2p

SW2#sh spanning-tree vlan 1
    VLAN0001
      Spanning tree enabled protocol ieee
      Root ID    Priority    32769
                 Address     000b.be78.8300
                 This bridge is the root
                 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                 Address     000b.be78.8300
                 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                 Aging Time 300

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/19           Desg FWD 19        128.19   P2p
```

- In this lab here, SW2 is the default root bridge. Configure SW1 to use the prority value of 4096 to ensure that SW1 should become Root Bridge.

```
SW1(config)#spanning-tree vlan 1 priority 4096
SW1(config)#exit

SW1#sh spanning-tree vlan 1
    VLAN0001
      Spanning tree enabled protocol ieee
      Root ID    Priority    4097
                 Address     000b.bee2.fa00
                 This bridge is the root
                 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
                 Address     000b.bee2.fa00
                 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                 Aging Time 15

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/1            Desg FWD 19        128.1    Edge P2p
    Fa0/19           Desg FWD 19        128.19   P2p
```

TASK:

- Configure SW1 so that STP logically blocks Ethernet links connected to SW2 if any of port on SW2 tries to become Root Bridge for any VLAN.

```
SW1(config)#int f0/19
SW1(config-if)#spanning-tree guard root
SW1(config-if)#exit
```

```
SW1#sh spanning-tree int f0/19 detail
 Port 19 (FastEthernet0/19) of VLAN0001 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.19.
   Designated root has priority 4097, address 000b.bee2.fa00
   Designated bridge has priority 4097, address 000b.bee2.fa00
   Designated port id is 128.19, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Root guard is enabled on the port
   BPDU: sent 68, received 194
```

Although Root Guard is enabled at the port level, it works on a per-VLAN basis.

TASK: Testing Root guard

- Configure sw2 with prority value of 0 to ensure that SW2 sends superior BPDU to sw1

```
SW2 (config)#spanning-tree vlan 1 priority 0
```

```
SW1#sh spanning-tree vlan 1
 VLAN0001
   Spanning tree enabled protocol ieee
   Root ID    Priority    4097
              Address     000b.bee2.fa00
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

   Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
              Address     000b.bee2.fa00
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

 Interface        Role Sts Cost      Prio.Nbr Type
 ---------------- ---- --- --------- -------- --------------------------------
 Fa0/1            Desg FWD 19        128.1    Edge P2p
 Fa0/19           Desg BKN*19        128.19   P2p *ROOT_Inc
```

SW1 no longer sends BPDUs outbound on its Root Inconsistentport,

TASK: Remove the priority configuration on SW2 and ensuure that sw2 uses the default proirity values

SW2 (config) #no spanning-tree vlan 1 priority 0

SW1#sh spanning-tree vlan 1

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     000b.bee2.fa00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     000b.bee2.fa00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    Edge P2p
Fa0/19           Desg LIS 19        128.19   P2p
```

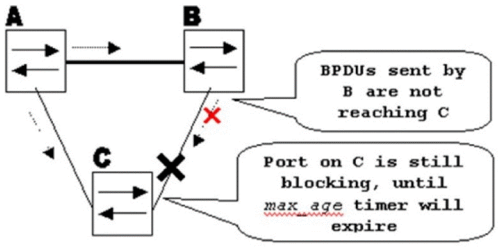
When superior BPDUs are no longer received, SW1 will start to send BPDUs outbound on the ports to negotiate the STP state and role;

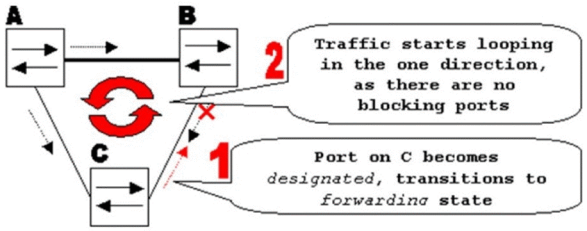
SW1#sh spanning-tree vlan 1

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     000b.bee2.fa00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     000b.bee2.fa00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    Edge P2p
Fa0/19           Desg FWD 19        128.19   P2p
```

Unidirectional link failure

- links for which one of the two transmission paths on the link has failed, but not both.
- This can happen as a result of miscabling, cutting one fiber cable, unplugging one fiber or other reasons.
- no longer receives STP BPDUs
- Still link forwards Traffic.
- blocking port from the alternate or backup port becomes designated and moves to a forwarding state. This situation creates a loop.
- This is called a unidirectional link





Unidirectional link failure

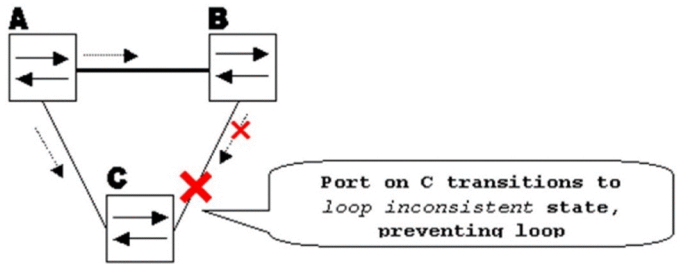
Solution:

Loopguard

UDLD

LOOP GAURD

- Stops the loops which can occur because of unidirectional link failures.
- prevents switch ports from wrongly moving from a blocking to a forwarding state when a unidirectional link exists in the network.



Loop Guard Configuration

On all point to point links

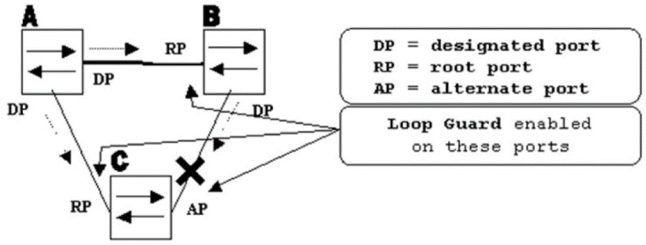
(config-if)**#spanning-tree guard loop default**

OR

On Specific links

(config)**#interface f0/20**

(config-if)**#spanning-tree guard loop**



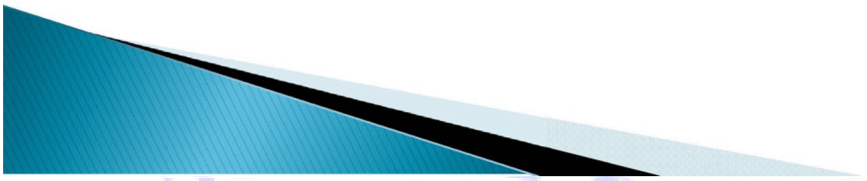
Loopguard automatically re-enables the port if it starts receiving BPDU again

Unidirectional Link Detection

- Do the same job as loop guard
- Designed more specific for fiber ports (can also work for UTP)
- detects a unidirectional link by sending periodic hellos out to the interface.
- It also uses probes, which must be acknowledged by the device on the other end of the link.

UDLD has two modes: normal and aggressive.

- **normal mode,** the link status is changed to Undetermined State if the hellos are not returned.
- **Aggressive mode**, the port is error-disabled if a unidirectional link is found. Aggressive mode is the recommended way to configure UDLD.



Unidirectional Link Detection

To enable UDLD on all fiber-optic interfaces, use the following command:
(config)# udld [enable | aggressive]

Note :
Although this command is given at global config mode, it applies only to fiber ports.
To enable UDLD on nonfiber ports, give the same command at interface config mode.
To control UDLD on a specific fiber port, use the following command:
(config-if)# udld port {aggressive | disable}

To reenable all interfaces shut by UDLD, use the following:
 # udld reset
To verify UDLD status, use the following:
 # show udld interface

UDLP & loop guard

Functionality	Loop Guard	UDLD
Configuration	Per-port	Per-port
Action granularity	Per-VLAN	Per-port
Auto-recover	Yes	Yes, with err-disable timeout feature
Protection against STP failures caused by unidirectional links	Yes, when enabled on all root and alternate ports in redundant topology	Yes, when enabled on all links in redundant topology
Protection against STP failures caused by problems in the software (designated switch does not send BPDU)	Yes	No
Protection against mis-wiring.	No	Yes

Err-Disable & Err-disable recovery

- the port is automatically disabled by the switch operating system software because of an error condition that is encountered on the port.
- When a port is error disabled, it is effectively shut down and no traffic is sent or received on that port.
- The port LED is set to the color orange

#Show interfaces gigabitethernet 4/1 status

Port Name	Status	Vlan	Duplex	Speed	Type
Gi4/1	err-disabled	100	full	1000	1000BaseSX

 # show interface gigabit4/1
GigabitEthernet4/1 is down, line protocol is down (**err-disabled**)

Err-disable recovery

Reasons for error disable state :

- Duplex Mismatch
- Loopback Error
- Link Flapping (up/down)
- Port Security Violation
- Unicast Flooding
- UDLD Failure
- Broadcast Storms
- BPDU Guard

Err-disable recovery

1. To recover a port that is in an Errdisable state, administrator must access the switch and configure the specific port with '**shutdown**' followed by the '**no shutdown**' command.
2. Use Err-disable recovery option

Errdisable recovery

choose the type of errors that automatically reenable the ports after a specified amount of time.

#show errdisable recovery

ErrDisable Reason	Timer Status
udld	Disabled
bpduguard	Disabled
security-violatio	Disabled
channel-misconfig	Disabled
pagp-flap	Disabled
dtp-flap	Disabled
link-flap	Disabled
l2ptguard	Disabled
psecure-violation	Disabled
gbic-invalid	Disabled
dhcp-rate-limit	Disabled
mac-limit	Disabled
unicast-flood	Disabled
arp-inspection	Disabled

Timer interval: 300 seconds

#errdisable recovery cause ?

all	Enable timer to recover from all causes
arp-inspection	Enable timer to recover from arp inspection error disable state
bpduguard	Enable timer to recover from BPDU Guard error disable state
channel-misconfig	Enable timer to recover from channel misconfig disable state
dhcp-rate-limit	Enable timer to recover from dhcp-rate-limit error disable state
dtp-flap	Enable timer to recover from dtp-flap error disable state
gbic-invalid	Enable timer to recover from invalid GBIC error disable state
l2ptguard	Enable timer to recover from l2protocol-tunnel error disable state
link-flap	Enable timer to recover from link-flap error disable state
mac-limit	Enable timer to recover from mac limit disable state
pagp-flap	Enable timer to recover from pagp-flap error disable state
psecure-violation	Enable timer to recover from psecure violation disable state
security-violation	Enable timer to recover from 802.1x violation disable state
udld	Enable timer to recover from udld error disable state
unicast-flood	Enable timer to recover from unicast flood disable state

(Config)**#errdisable recovery cause bpduguard**
(Config)**#errdisable recovery interval 120**

Errdisable autorecovery

To enable the Errdisable autorecovery feature for all supported reasons
(config)**# errdisable recovery cause all**

show interfaces status err-disabled

- Shows which local ports are involved in the errdisabled state.

show errdisable recovery

- Shows the time period after which the interfaces are enabled for errdisable conditions.

show errdisable detect

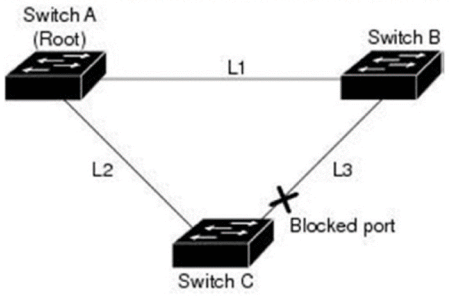
- Shows the reason for the errdisable status.

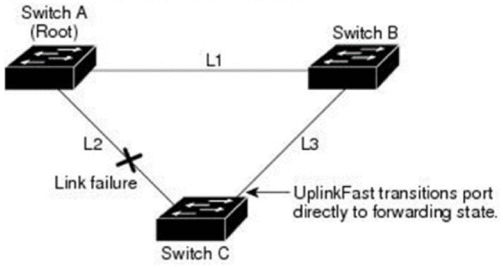
STP Flavours

RSTP, PVSTP, CST, MSTP

Spanning-tree uplink fast

- Legacy / Cisco proprietary feature
- Uplink Fast is for speeding convergence when a direct link to an upstream switch fails.
- When uplinkfast is enabled, it is enabled for the entire switch and all VLANs





SW1(config)#**spanning-tree uplinkfast**

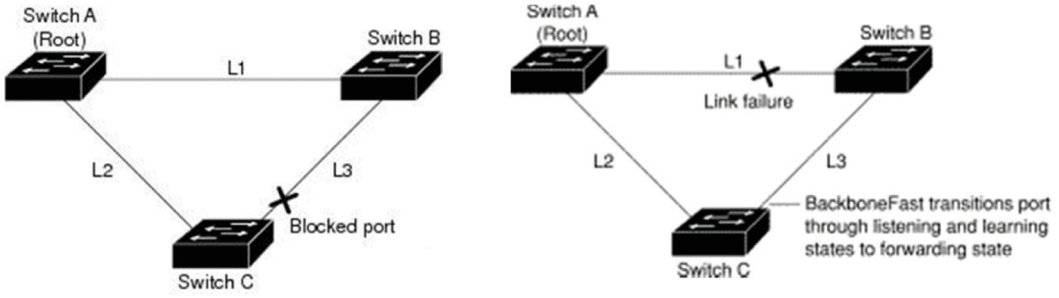
SW1# show spanning-tree

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    8193
             Address     0016.4748.dc80
             Cost        3019
             Port        130 (FastEthernet3/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    49152
             Address     0009.b6df.c401
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  Uplinkfast enabled
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa3/1            Altn BLK 3019      128.129  P2p
Fa3/2            Root FWD 3019      128.130  P2p
```

NOTE :

- This command is not allowed on root bridge switch.
- When UplinkFast is configured, the bridge priority is changed to 49,152 so that this switch will not be selected as root.

Spanning-tree Backbonefast



- Legacy / Cisco proprietary feature
- Backbone Fast can reduce the maximum convergence delay only from 50 to 30 seconds.

Spanning-tree Backbonefast configuration

To configure BackboneFast,

Switch(config)# **spanning-tree backbonefast**

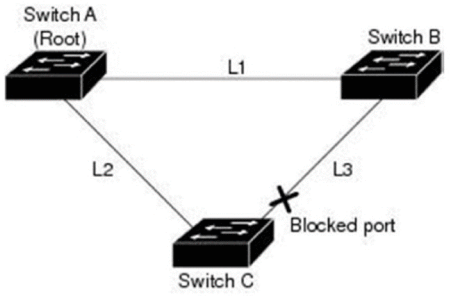
To verify

Switch# **show spanning-tree backbonefast**

BackboneFast is enabled

Rapid STP (RSTP) 802.1w

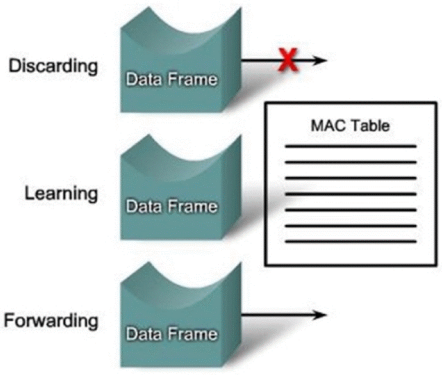
- 802.1w is a standards way of speeding STP convergence.
- Inbuilt features of portfast, uplinkfast, backbonefast.
- Path Calculation remains same as STP.



RSTP port States

Comparing 802.1d and 802.1w Port States

STP Port State	Equivalent RSTP Port State
Disabled	Discarding
Blocking	Discarding
Listening	Discarding
Learning	Learning
Forwarding	Forwarding

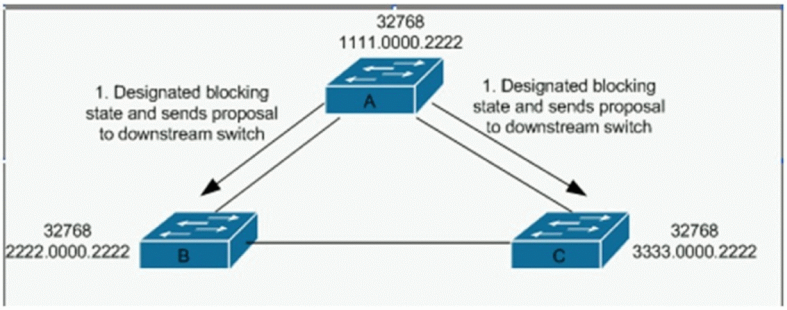


Discarding - Frames are dropped, no addresses are learned. (link down / blocking/during sync)

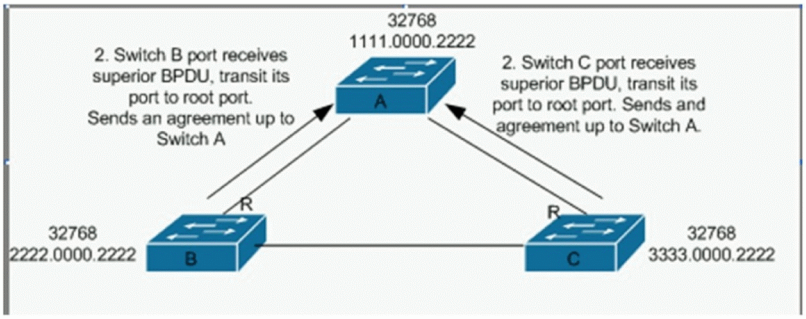
Learning - Frames are dropped, but addresses are learned.

Forwarding - Frames are forwarded

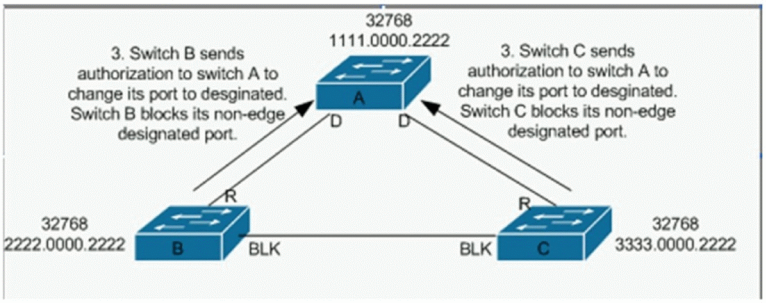
RSTP Synchronization

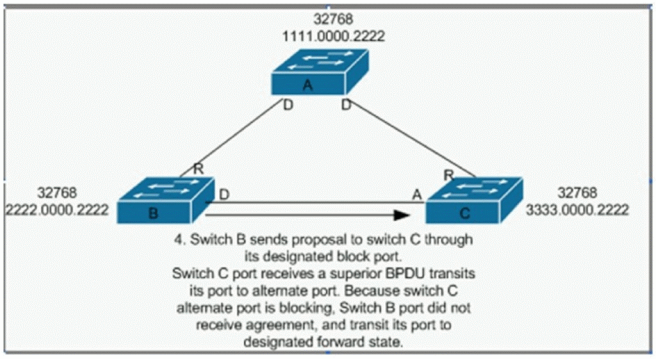


SWA assumes its port is designated and sends out a proposal. SWB will agree to this proposal.



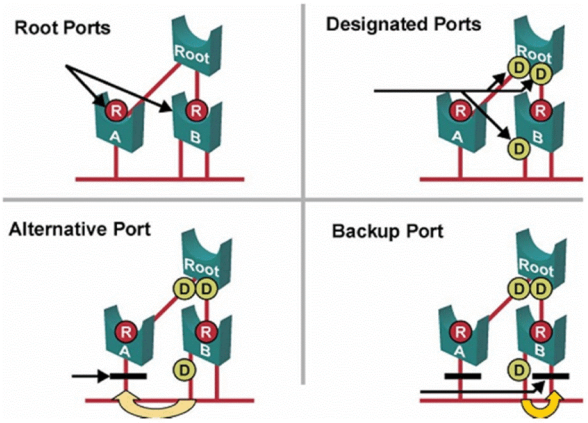
RSTP Synchronization





RSTP port roles

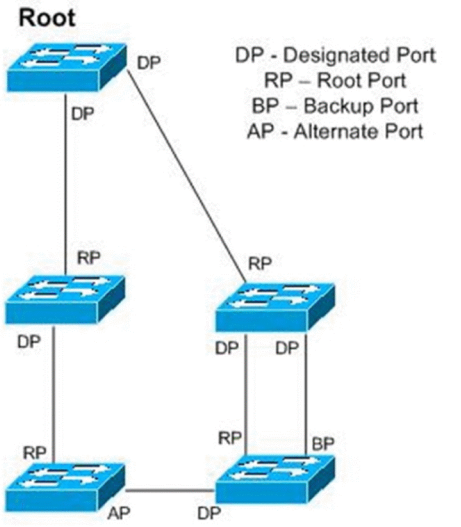
Root port:	The best path to the root (same as STP)
Designated port:	Same role as with STP
Alternate port:	A backup to the root port
Backup port:	A backup to the designated port
Disabled port:	Not used in the Spanning Tree
Edge port:	Connected only to an end user



RSTP port roles (Contd)

Alternate port:

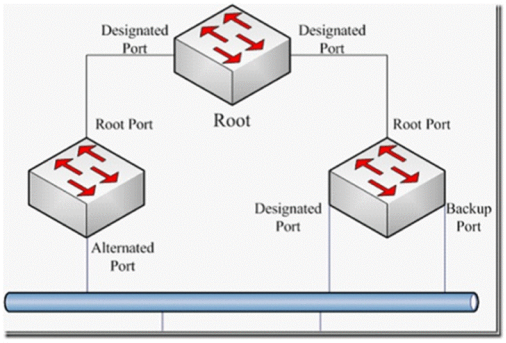
- A backup to the root port
- Less desirable path to the root
- Operates in discarding state.
- Same as uplinkfast (legacy)



RSTP port roles (Contd)

Backup port:

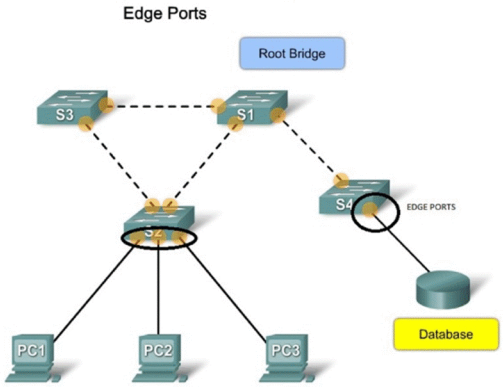
- The backup port applies only when a single switch has two links to the same segment (collision domain).
- To have two links to the same collision domain, the switch must be attached to a hub.
- A backup to the designated port
- Multiple links attached to the same network segment
- Activates if primary designated fails.



RSTP port roles (Contd)

Edge port:

- Equivalent to portfast in STP.
- Connected only to an end user .
- Maintain edge status as long as no BPDU received (with BPDU filter) .



BPDU Differences in RSTP

- In regular STP, BPDUs are originated by the root and relayed by each switch.
- In RSTP, each switch originates BPDUs, whether or not it receives a BPDU on its root port. PVST is done by Rapid PVST+ on Catalyst switches.
- Hello= 2 sec , Dead = 6 sec

RSTP Configuration

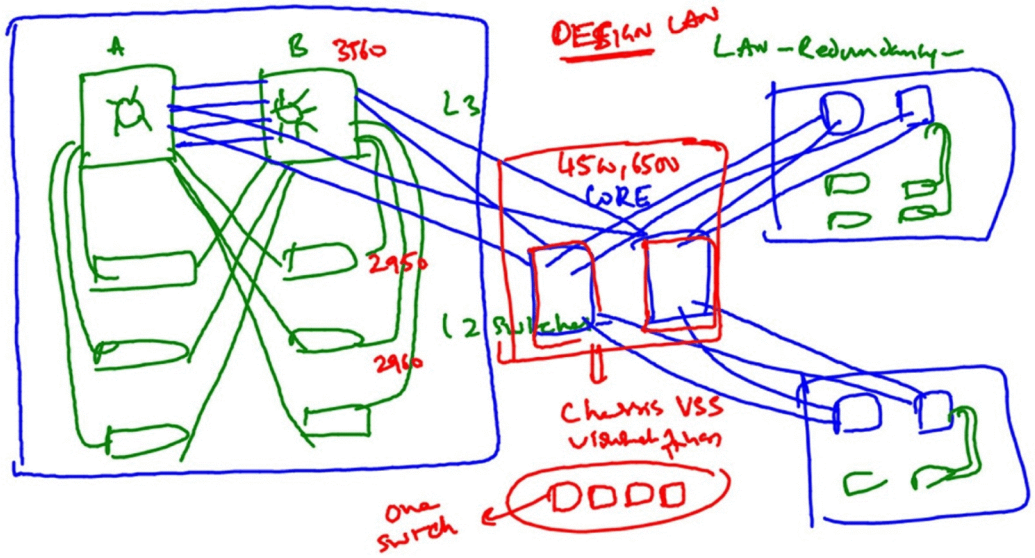
(config)**#spanning-tree mode rapid-pvst**

```
#sh spanning-tree
      VLAN0001
        Spanning tree enabled protocol rstp
        Root ID    Priority    32769
                   Address     0001.C9A4.567D
                   Cost        19
                   Port        20(FastEthernet0/20)
                   Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

        Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                   Address     000A.414A.42D8
                   Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                   Aging Time  20

      Interface        Role Sts Cost      Prio.Nbr Type
      ---------------- ---- --- --------- -------- --------------------------------
      Fa0/20           Root LSN 19        128.20   P2p
```

RSTP port costs

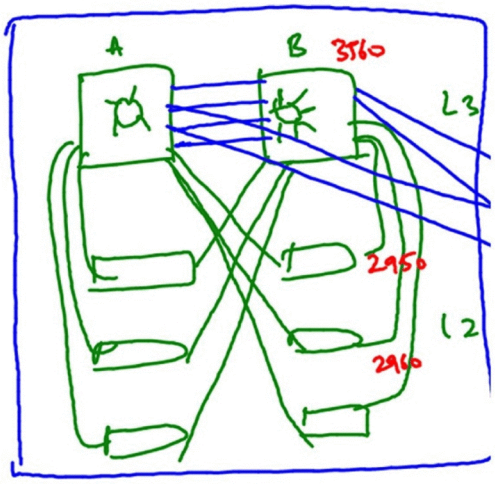
Data rate	STP Cost (802.1D-1998)	RSTP Cost (802.1W-2001)
4 Mbit/s	250	5,000,000
10 Mbit/s	100	2,000,000
16 Mbit/s	62	1,250,000
100 Mbit/s	19	200,000
1 Gbit/s	4	20,000
2 Gbit/s	3	10,000
10 Gbit/s	2	2,000

Hierarchical Campus Model



STP : Selecting Root Bridge

- Default root bridge election : **priority + Base Mac**
- Recommended to Select high speed Switch to be elected as Root Bridge .
  1. **Change priority**
  2. **Primary / Secondary**



STP : Selecting Root Bridge Configuration

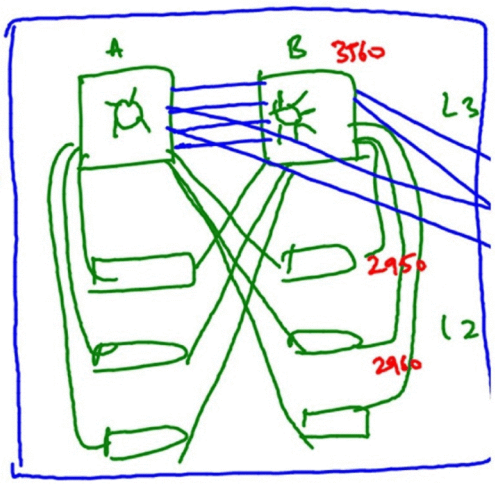
SW-A(config)#spanning-tree vlan 1 **root Primary**

SW-B(config)#spanning-tree vlan 1 **root Secondary**

OR

SW-A(config)#spanning-tree vlan 1 **priority 0**

SW-B(config)#spanning-tree vlan 1 **priority 4096**



NOTE :

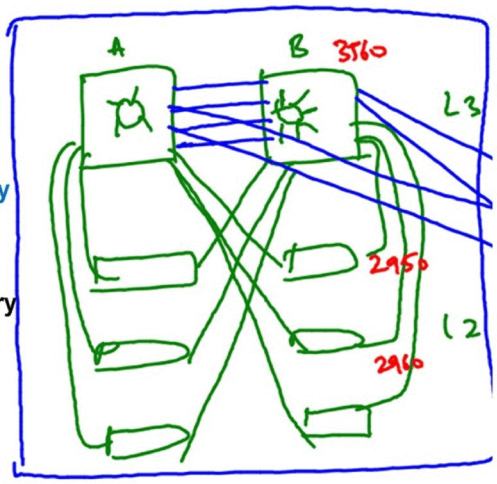
- Priority values can be only multiples of 4096
- Primary reduces priority by 8192 from default priority
- secondary reduces priority 4096 from default priority

Per Vlan STP

- every vlan runs a separate STP instance.
- Cisco proprietary. (PVST supports only ISL)
- PVST+ allows interoperability between CST and PVST in Cisco switches and support the IEEE 802.1Q standard.
- Provides load sharing
- More overhead

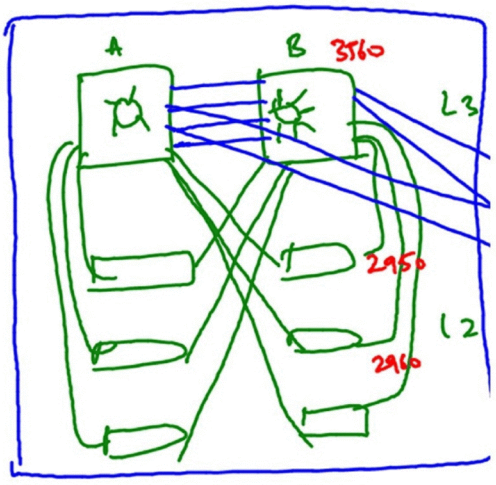
A(config)#spanning-tree vlan 10,20 root primary
B(config)#spanning-tree vlan 30.40 root secondary

A(config)#spanning-tree vlan 10.20 root secondary
B(config)#spanning-tree vlan 30,40 root primary



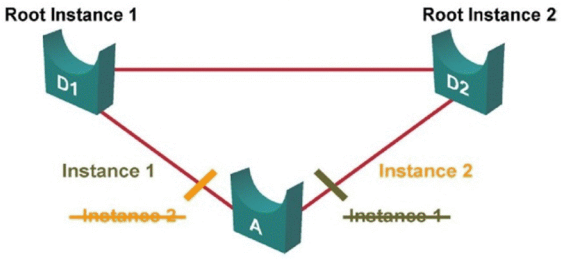
Common STP (CST)

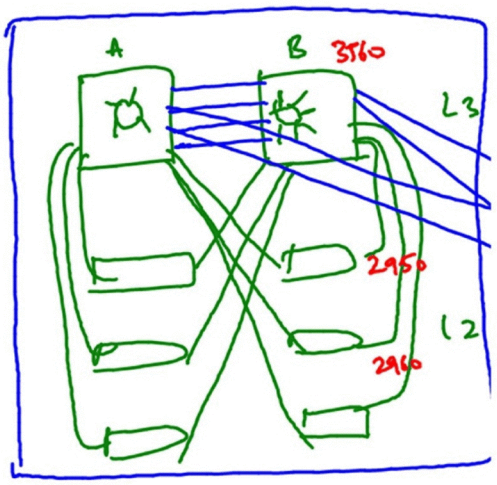
- Runs on spanning-tree instance for all Vlans
- reduces CPU load
- No load sharing



Multiple Spanning Tree (MST)

- Started as Cisco's MISTP
- Originally standard defined in IEEE 802.1s
- allows several VLANs to be mapped to single instance of STP
- reduces number of spanning-tree instances (processing overhead).
- instance handles multiple VLANs that have the same Layer 2 topology.



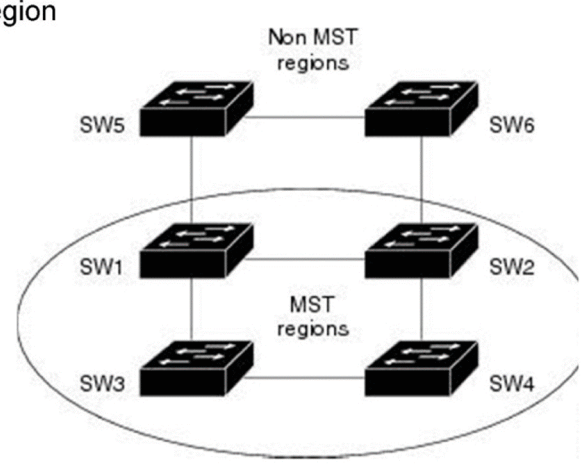


Instance 1 maps to VLANs 1–500
Instance 2 maps to VLANs 501–1000

MSTP Regions

collection of switches that have the same MST configuration comprises an MST region

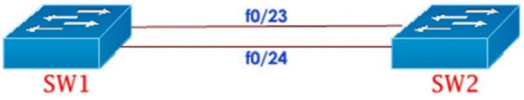
1. Instance name (32 bytes)
2. Revision number (two bytes)
3. VLAN to STP instance mappings



MSTP Configuration

SW1 /SW2

SWx(config)**#spanning-tree mode mst**
SWx(config)# **spanning-tree mst configuration**
SWx(config-mst)# **revision 1**
SWx(config-mst)# **name CCIE**
SWx(config-mst)# **instance 1 vlan 10,20**
SWx(config-mst)# **instance 2 vlan 30,40**
SWx(config-mst)# **exit**



SW1(config)**#spanning-tree mst 1 root primary**
SW1(config)**#spanning-tree mst 2 root secondary**

SW2 (config)**#spanning-tree mst 2 root primary**
SW2 (config)**#spanning-tree mst 1 root secondary**

NOTE:

- an instance must have the same MST name and revision number
- If not matches then they are considered as different instances and not the same, even if the instances contain the same vlans.

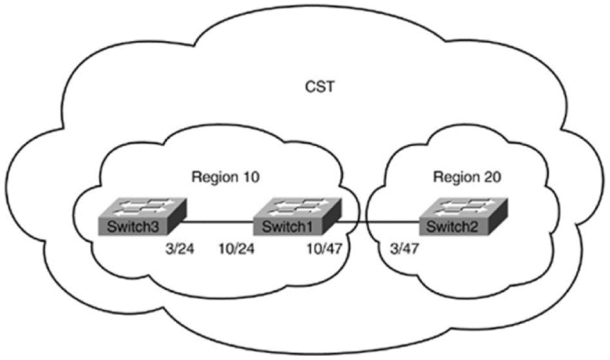
Intra vs Inter Region

Intra Region

- Details of the region are known within the region
- VLAN to STPIs are manually defined
- Undefined VLANs fall into CIST (MST 0)

Inter Region

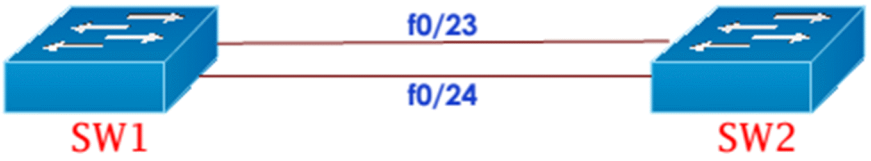
- Details between regions are not known
- Different regions see each other as virtual bridges
- Result is simplified Inter-Region calculation
- Intra-region MSTIs are collapsed into CIST



MST Interoperability

- MST is backwards compatible with legacy CST and PVST+
- Behaves like Inter-Region MST
- CST Root must be within MST domain

LAB: MSTP (MULTILPLE SPANNING-TREE)



SW1#sh cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
SW2	Fas 0/24	165	S I	WS-C3560-	Fas 0/24
SW2	Fas 0/23	165	S I	WS-C3560-	Fas 0/23

TASK:

- Configure manual trunk between sw1 and sw2 connected links
- Configure vtp to synchronize the vlan information between two switches
- Create vlan 10, 20 , 30 , 40 on any one of the switch

SW1/SW2

```
SWx(config)#int range f0/23 - 24
SWx(config-if-range)#switchport trunk encapsulation dot1q
SWx(config-if-range)#switchport mode trunk
SWx(config-if-range)#switchport nonegotiate
SWx(config-if-range)#end

SWx(config)#vtp domain CCIE
```

SW1 or SW2

```
SW1(config)#vlan 10
SW1(config-vlan)#vlan 20
SW1(config-vlan)#vlan 30
SW1(config-vlan)#vlan 40
SW1(config-vlan)#end

SW1#sh spanning-tree vlan 10
    VLAN0010
      Spanning tree enabled protocol ieee
      Root ID    Priority    32778
```

```
            Address     0017.95db.9700
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
            Address     0017.95db.9700
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Desg FWD 19        128.25   P2p
        Fa0/24           Desg FWD 19        128.26   P2p


SW1#sh spanning-tree vlan 20
        VLAN0020
          Spanning tree enabled protocol ieee
          Root ID    Priority    32788
            Address     0017.95db.9700
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
            Address     0017.95db.9700
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Desg FWD 19        128.25   P2p
        Fa0/24           Desg FWD 19        128.26   P2p

SW1#sh spanning-tree vlan 30
        VLAN0030
          Spanning tree enabled protocol ieee
          Root ID    Priority    32798
            Address     0017.95db.9700
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
            Address     0017.95db.9700
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Aging Time 300 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	Desg	FWD	19	128.25	P2p
Fa0/24	Desg	FWD	19	128.26	P2p

SW1#sh spanning-tree vlan 40

VLAN0040
Spanning tree enabled protocol ieee
Root ID Priority 32808
Address 0017.95db.9700
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32808 (priority 32768 sys-id-ext 40)
Address 0017.95db.9700
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	Desg	FWD	19	128.25	P2p
Fa0/24	Desg	FWD	19	128.26	P2p

- From the above outputs we can see that the SW1 is the default root bridge for all the Vlan created

To verify the base mac address of the switch

SW1#sh version | in ethernet
Base ethernet MAC Address : 00:17:95:DB:97:00

SW2#sh version | in ethernet
Base ethernet MAC Address : 00:23:AC:E6:C7:80

SW2#sh spanning-tree root

Vlan	Root ID	Root Cost	Hello Time	Max Age	Fwd Dly	Root Port
VLAN0001	32769 0017.95db.9700	19	2	20	15	Fa0/23
VLAN0010	32778 0017.95db.9700	19	2	20	15	Fa0/23
VLAN0020	32788 0017.95db.9700	19	2	20	15	Fa0/23
VLAN0030	32798 0017.95db.9700	19	2	20	15	Fa0/23

```
VLAN0040        32808 0017.95db.9700       19    2   20  15  Fa0/23
```

SW2#sh spanning-tree bridge

```
                                        Hello  Max  Fwd
Vlan                 Bridge ID          Time  Age  Dly  Protocol
---------------- ---------------------------------- -----  ---  ---  --------
VLAN0001         32769 (32768,  1) 0023.ace6.c780    2    20   15  ieee
VLAN0010         32778 (32768, 10) 0023.ace6.c780    2    20   15  ieee
VLAN0020         32788 (32768, 20) 0023.ace6.c780    2    20   15  ieee
VLAN0030         32798 (32768, 30) 0023.ace6.c780    2    20   15  ieee
VLAN0040         32808 (32768, 40) 0023.ace6.c780    2    20   15  ieee
```

SW2#sh spanning-tree vlan 10

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0017.95db.9700
             Cost        19
             Port        25 (FastEthernet0/23)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority    32778 (priority 32768 sys-id-ext 10)
             Address     0023.ace6.c780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/23           Root FWD 19        128.25   P2p
Fa0/24           Altn BLK 19        128.26   P2p
```


TASK:

Configure MSTP on both switches

- With vlan 10 and 20 in MST instance 1
- With vlan 30 and 40 in MST instance 2
- And the remaining and future vlans should be present in default instance (MST 0)
- Revision number should be 1 and region name should be CCIE
- SW1 should be root bridge for MST 1
- SW2 should be root bridge for MST 2
- Defaut instance MST 0 should have the default root bridge (SW1 in our lab)

SW1 /SW2

```
SWx(config)#spanning-tree mode mst
```

```
SWx(config)#  spanning-tree mst configuration
SWx(config-mst)#  revision 1
SWx(config-mst)#  name CCIE
SWx(config-mst)#  instance 1 vlan 10,20
SWx(config-mst)#  instance 2 vlan 30,40
SWx(config-mst)#  exit

SW1#sh spanning-tree mst configuration
        Name      [CCIE]
        Revision  1     Instances configured 3

        Instance  Vlans mapped
        --------  ---------------------------------------------------------------------
        0         1-9,11-19,21-29,31-39,41-4094
        1         10,20
        2         30,40
        -------------------

SW2#sh spanning-tree

        MST0
          Spanning tree enabled protocol mstp
          Root ID    Priority    32768
                     Address     0017.95db.9700
                     Cost        0
                     Port        25 (FastEthernet0/23)
                     Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
                     Address     0023.ace6.c780
                     Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Root FWD 200000    128.25   P2p
        Fa0/24           Altn BLK 200000    128.26   P2p


        MST1
          Spanning tree enabled protocol mstp
          Root ID    Priority    32769
                     Address     0017.95db.9700
                     Cost        200000
```

```
              Port        25 (FastEthernet0/23)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0023.ace6.c780
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/23           Root FWD 200000    128.25   P2p
Fa0/24           Altn BLK 200000    128.26   P2p


MST2
  Spanning tree enabled protocol mstp
  Root ID    Priority    32770
              Address     0017.95db.9700
              Cost        200000
              Port        25 (FastEthernet0/23)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32770  (priority 32768 sys-id-ext 2)
              Address     0023.ace6.c780
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/23           Root FWD 200000    128.25   P2p
Fa0/24           Altn BLK 200000    128.26   P2p


SW1#sh spanning-tree mst 1
      ##### MST1    vlans mapped:   10,20
      Bridge        address 0017.95db.9700  priority      32769 (32768 sysid 1)
      Root          this switch for MST1

      Interface        Role Sts Cost      Prio.Nbr Type
      ---------------- ---- --- --------- -------- --------------------------------
      Fa0/23           Desg FWD 200000    128.25   P2p
      Fa0/24           Desg FWD 200000    128.26   P2p

SW1#sh spanning-tree mst 2
      ##### MST2    vlans mapped:   30,40
      Bridge        address 0017.95db.9700  priority      32770 (32768 sysid 2)
```

Root this switch for MST2

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	Desg	FWD	200000	128.25	P2p
Fa0/24	Desg	FWD	200000	128.26	P2p

SW1#sh spanning-tree mst 0

MST0 vlans mapped: 1-9,11-19,21-29,31-39,41-4094
Bridge address 0017.95db.9700 priority 32768 (32768 sysid 0)
Root this switch for the CIST
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured hello time 2 , forward delay 15, max age 20, max hops 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	Desg	FWD	200000	128.25	P2p
Fa0/24	Desg	FWD	200000	128.26	P2p

From the above, by default SW1 becomes the root bridge for all the MST instances created Even we can verify using command # sh spanning-tree root command

SW1#sh spanning-tree root

MST Instance	Root ID	Root Cost	Hello Time	Max Age	Fwd Dly	Root Port
MST0	32768 0017.95db.9700	0	2	20	15	
MST1	32769 0017.95db.9700	0	2	20	15	
MST2	32770 0017.95db.9700	0	2	20	15	

SW1#sh spanning-tree bridge

MST Instance	Bridge ID	Hello Time	Max Age	Fwd Dly	Protocol
MST0	32768 (32768, 0) 0017.95db.9700	2	20	15	mstp
MST1	32769 (32768, 1) 0017.95db.9700	2	20	15	mstp
MST2	32770 (32768, 2) 0017.95db.9700	2	20	15	mstp

SW2#sh spanning-tree bridge

MST Instance	Bridge ID	Hello Time	Max Age	Fwd Dly	Protocol
MST0	32768 (32768, 0) 0023.ace6.c780	2	20	15	mstp

```
MST1            32769 (32768,  1) 0023.ace6.c780    2    20   15  mstp
MST2            32770 (32768,  2) 0023.ace6.c780    2    20   15  mstp
SW2#sh spanning-tree root
                                        Root    Hello Max Fwd
MST Instance          Root ID           Cost    Time  Age Dly  Root Port
---------------- -------------------- --------- ----- --- ---  ------------
MST0            32768 0017.95db.9700         0    2   20  15  Fa0/23
MST1            32769 0017.95db.9700    200000    2   20  15  Fa0/23
MST2            32770 0017.95db.9700    200000    2   20  15  Fa0/23
```

TASK

- SW1 should be root bridge for MST 1
- SW2 should be root bridge for MST 2
- Defaut instance MST 0 should have the default root bridge (SW1 in our lab)

```
SW1(config)#spanning-tree mst 1 priority 0
SW1(config)#spanning-tree mst 2 priority 4096

SW2(config)#spanning-tree mst 2 priority 0
SW2(config)#spanning-tree mst 1 priority 4096
```

OR

```
SW1(config)#spanning-tree mst 1 root primary
SW1(config)#spanning-tree mst 2 root secondary

SW2 (config)#spanning-tree mst 2 root primary
SW2 (config)#spanning-tree mst 1 root secondary
```

In this example I used changing the priority value (first one)

```
SW1#sh spanning-tree MST 1
#####  MST1    vlans mapped:   10,20
Bridge        address 0017.95db.9700  priority      1     (0 sysid 1)
Root          this switch for MST1

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/23           Desg FWD 200000    128.25   P2p
Fa0/24           Desg FWD 200000    128.26   P2p

SW1#sh spanning-tree mst 2
#####  MST2    vlans mapped:   30,40
Bridge        address 0017.95db.9700  priority      4098  (4096 sysid 2)
Root          address 0023.ace6.c780  priority      2     (0 sysid 2)
```

```
                port    Fa0/23          cost         200000    rem hops 19

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Root FWD 200000    128.25   P2p
        Fa0/24           Altn BLK 200000    128.26   P2p
```

SW1#sh spanning-tree root

```
                                        Root    Hello Max Fwd
        MST Instance          Root ID         Cost    Time  Age Dly  Root Port
        ---------------- -------------------- --------- ----- --- ---  ------------
        MST0            32768 0017.95db.9700         0    2   20  15
        MST1             1 0017.95db.9700         0    2   20  15
        MST2             2 0023.ace6.c780    200000    2   20  15  Fa0/23
```

SW2#sh spanning-tree mst 2

```
        ##### MST2    vlans mapped:   30,40
        Bridge        address 0023.ace6.c780  priority      2     (0 sysid 2)
        Root          this switch for MST2

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Desg FWD 200000    128.25   P2p
        Fa0/24           Desg FWD 200000    128.26   P2p
```

SW2#sh spanning-tree mst 1

```
        ##### MST1    vlans mapped:   10,20
        Bridge        address 0023.ace6.c780  priority      4097  (4096 sysid 1)
        Root          address 0017.95db.9700  priority      1     (0 sysid 1)
                      port    Fa0/23          cost          200000    rem hops 19

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Root FWD 200000    128.25   P2p
        Fa0/24           Altn BLK 200000    128.26   P2p
```

SW2#sh spanning-tree root

```
                                        Root    Hello Max Fwd
        MST Instance          Root ID         Cost    Time  Age Dly  Root Port
        ---------------- -------------------- --------- ----- --- ---  ------------
        MST0            32768 0017.95db.9700         0    2   20  15  Fa0/23
        MST1             1 0017.95db.9700    200000    2   20  15  Fa0/23
        MST2             2 0023.ace6.c780         0    2   20  15
```

```
SW2#sh spanning-tree bridge
                                        Hello  Max  Fwd
MST Instance          Bridge ID          Time  Age  Dly  Protocol
---------------- --------------------------------- -----  ---  ---  --------
MST0          32768 (32768,   0) 0023.ace6.c780    2    20   15  mstp
MST1           4097 ( 4096,   1) 0023.ace6.c780    2    20   15  mstp
MST2              2 (    0,   2) 0023.ace6.c780    2    20   15  mstp
```

TASK:

- configure SW2 to make sure that F0/24 of SW2 is fwd for MST1
- configure SW1 to make sure that F0/24 of SW1 is fwd for MST2

```
SW2#sh spanning-tree mst 1
        ##### MST1    vlans mapped:   10,20
        Bridge        address 0023.ace6.c780  priority      4097  (4096 sysid 1)
        Root          address 0017.95db.9700  priority      1     (0 sysid 1)
                      port    Fa0/23          cost          200000    rem hops 19

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Root FWD 200000    128.25   P2p
        Fa0/24           Altn BLK 200000    128.26   P2p

SW2(config)#int f0/24
SW2(config-if)#spanning-tree mst 1 cost ?
  <1-200000000>  Change the interface spanning tree path cost for an instance

SW2(config-if)#spanning-tree mst 1 cost 1000
SW2(config-if)#end

SW2#sh spanning-tree mst 1
        ##### MST1    vlans mapped:   10,20
        Bridge        address 0023.ace6.c780  priority      4097  (4096 sysid 1)
        Root          address 0017.95db.9700  priority      1     (0 sysid 1)
                      port    Fa0/24          cost          1000      rem hops 19

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Altn BLK 200000    128.25   P2p
        Fa0/24           Root FWD 1000      128.26   P2p

SW1#sh spanning-tree mst 2
        ##### MST2    vlans mapped:   30,40
```

```
        Bridge        address 0017.95db.9700  priority      4098  (4096 sysid 2)
        Root          address 0023.ace6.c780  priority      2     (0 sysid 2)
                      port    Fa0/23          cost          200000    rem hops 19

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Root FWD 200000    128.25   P2p
        Fa0/24           Altn BLK 200000    128.26   P2p
```

```
SW1(config)#int f0/24
SW1(config-if)#spanning-tree mst 2 cost 1000
SW1(config-if)#end

SW1#sh spanning-tree mst  2
        ##### MST2    vlans mapped:   30,40
        Bridge        address 0017.95db.9700  priority      4098  (4096 sysid 2)
        Root          address 0023.ace6.c780  priority      2     (0 sysid 2)
                      port    Fa0/24          cost          1000      rem hops 19

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Altn BLK 200000    128.25   P2p
        Fa0/24           Root FWD 1000      128.26   P2p
```

TASK:

- Remove the previous task configs (cost from interface of SW1 and SW2 f0/24 port)
- Configure SW1 to make sure that F0/24 of SW2 is fwd for MST1
- Configure SW2 to make sure that F0/24 of SW1 is fwd for MST2

```
SW1(config)#int f0/24
SW1(config-if)#NO spanning-tree mst 2 cost 1000
SW1(config-if)#end

SW1#sh spanning-tree mst 2
        ##### MST2    vlans mapped:   30,40
        Bridge        address 0017.95db.9700  priority      4098  (4096 sysid 2)
        Root          address 0023.ace6.c780  priority      2     (0 sysid 2)
                      port    Fa0/23          cost          200000    rem hops 19

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Root FWD 200000    128.25   P2p
        Fa0/24           Altn BLK 200000    128.26   P2p

SW2(config)#int f0/24
```

```
SW2(config-if)#NO spanning-tree mst 1 cost 1000
SW2(config-if)#end


SW2#sh spanning-tree mst 1
        ##### MST1    vlans mapped:   10,20
        Bridge        address 0023.ace6.c780  priority      4097  (4096 sysid 1)
        Root          address 0017.95db.9700  priority      1     (0 sysid 1)
                      port    Fa0/23          cost          200000    rem hops 19

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Root FWD 200000    128.25   P2p
        Fa0/24           Altn BLK 200000    128.26   P2p

SW1#sh spanning-tree mst 1
        ##### MST1    vlans mapped:   10,20
        Bridge        address 0017.95db.9700  priority      1     (0 sysid 1)
        Root          this switch for MST1

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Desg FWD 200000    128.25   P2p
        Fa0/24           Desg FWD 200000    128.26   P2p
```

TASK: Configure SW1 to make sure that F0/24 of SW2 is fwd for MST1

```
SW1(config)#int f0/24
SW1(config-if)#spanning-tree mst 1 port-priority ?
  <0-240>  port priority in increments of 16

SW1(config-if)#spanning-tree mst 1 port-priority 0
SW1(config-if)#exit

SW1#sh spanning-tree mst 1
        ##### MST1    vlans mapped:   10,20
        Bridge        address 0017.95db.9700  priority      1     (0 sysid 1)
        Root          this switch for MST1

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/23           Desg FWD 200000    128.25   P2p
        Fa0/24           Desg FWD 200000      0.26   P2p
```

```
SW2#sh spanning-tree mst 1
      ##### MST1    vlans mapped:   10,20
      Bridge       address 0023.ace6.c780  priority      4097  (4096 sysid 1)
      Root         address 0017.95db.9700  priority      1     (0 sysid 1)
                   port    Fa0/24          cost          200000    rem hops 19

      Interface        Role Sts Cost      Prio.Nbr Type
      ---------------- ---- --- --------- -------- --------------------------------
      Fa0/23           Altn BLK 200000    128.25   P2p
      Fa0/24           Root FWD 200000    128.26   P2p
```

TASK: Configure SW2 to make sure that F0/24 of SW1 is fwd for MST2

```
SW2#sh spanning-tree mst  2
      ##### MST2    vlans mapped:   30,40
      Bridge       address 0023.ace6.c780  priority      2     (0 sysid 2)
      Root         this switch for MST2

      Interface        Role Sts Cost      Prio.Nbr Type
      ---------------- ---- --- --------- -------- --------------------------------
      Fa0/23           Desg FWD 200000    128.25   P2p
      Fa0/24           Desg FWD 200000    128.26   P2p

SW2(config)#int f0/24
SW2(config-if)#spanning-tree mst 2 port-priority 0
SW2(config-if)#end

SW2#sh spanning-tree mst  2
      ##### MST2    vlans mapped:   30,40
      Bridge       address 0023.ace6.c780  priority      2     (0 sysid 2)
      Root         this switch for MST2

      Interface        Role Sts Cost      Prio.Nbr Type
      ---------------- ---- --- --------- -------- --------------------------------
      Fa0/23           Desg FWD 200000    128.25   P2p
      Fa0/24           Desg FWD 200000      0.26   P2p

SW1#sh spanning-tree mst  2
      ##### MST2    vlans mapped:   30,40
      Bridge       address 0017.95db.9700  priority      4098  (4096 sysid 2)
      Root         address 0023.ace6.c780  priority      2     (0 sysid 2)
                   port    Fa0/24          cost          200000    rem hops 19
```

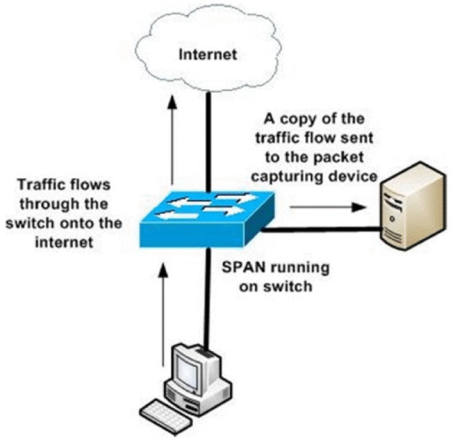
```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/23           Altn BLK 200000    128.25   P2p
Fa0/24           Root FWD 200000    128.26   P2p
```

Switch port Analyzer

SPAN, RSPAN, ERSPAN

SPAN

- Cisco Catalyst switches support a method of directing all traffic from a source port or source VLAN to a single port. This feature, called SPAN (for Switch Port Analyzer)



LAB-1 : SPAN

Mirror traffic sent or received from interface fa0/12 to interface fa0/24. All traffic sent or received on fa0/12 is sent to fa0/24.

```
SWITCH# configure terminal
SWITCH(config)# monitor session 1 source interface fa0/12
SWITCH(config)# monitor session 1 destination interface fa0/24
```

support three types of traffic:
transmitted, received, and both.

LAB-2 : SPAN

Configure a switch to send the following traffic to interface fa0/24, preserving the encapsulation from the sources:

1. **Received on interface fa0/18**
2. **Sent on interface fa0/9**
3. **Sent and received on interface fa0/19 (which is a trunk)**
4. **We also need to filter (remove) VLANs 1, 2, 3, and 229 from the traffic coming from the fa0/19 trunk port.**

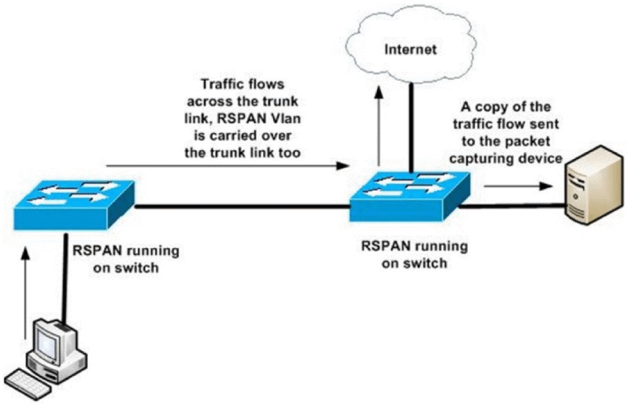
```
SWITCH# config term
SWITCH(config)# monitor session 11 source interface fa0/18 rx
SWITCH(config)# monitor session 11 source interface fa0/9 tx
SWITCH(config)# monitor session 11 source interface fa0/19
SWITCH(config)# monitor session 11 filter vlan 1 - 3 , 229
SWITCH(config)# monitor session 11 destination interface fa0/24
```

RSPAN

- The destination port for a SPAN session can be on the local switch, as in SPAN operation.

  Or

- it can be a port on another switch in the network. This mode is known as Remote SPAN, or RSPAN.

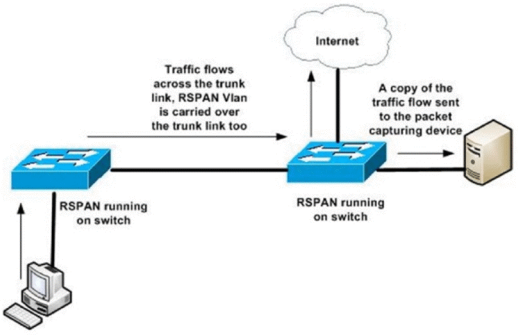


RSPAN Configuration

- specify that the new VLAN is an RSPAN VLAN
- RSPAN VLAN, can't be assigned to any access ports.
- Requires a separate RSPAN source session to be configured
- Separate RSPAN destination session to be configured.

This to check before Configuration :

- Trunking
- Trunk must allow remote-span Vlan
- VTP (optional)
- VTP if enabled (disable for remote span Vlan)



RSPAN : Lab-1

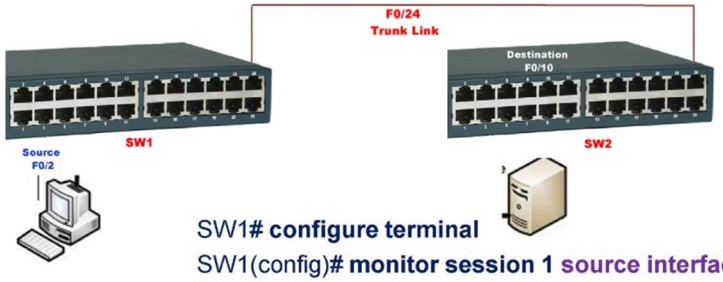
- specify that the new VLAN is an RSPAN VLAN
- RSPAN VLAN, can't be assigned to any access ports.

SW1/SW2

```
SWx# configure terminal
SWx(config)# vlan 199
SWx(config-vlan)# remote-span
SWx(config-vlan)# end

SWx# show vlan remote-span
Remote SPAN VLANs
------------------------
   200
```

RSPAN : Lab-1 (Contd)

- Requires a separate RSPAN source session to be configured
- Separate RSPAN destination session to be configured.




```
SW1# configure terminal
SW1(config)# monitor session 1 source interface fastEthernet0/2
rx
SW1(config)# monitor session 1 destination remote vlan 199
SW1(config)# exit

SW2# configure terminal
SW2(config)# monitor session 1 source remote vlan 199
SW2(config)# monitor session 1 destination interface
fastEthernet0/10
SW2(config)# exit
```

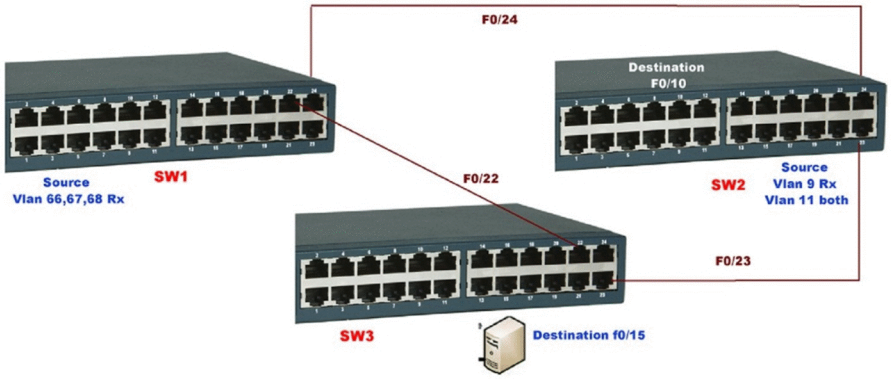
LAB : RSPAN

we need to configure two switches, SW1 and SW2, to send traffic to RSPAN VLAN 199, which is delivered to port fa0/24 on switch 3 as follows:

From SW1, all traffic received on VLANs 66–68

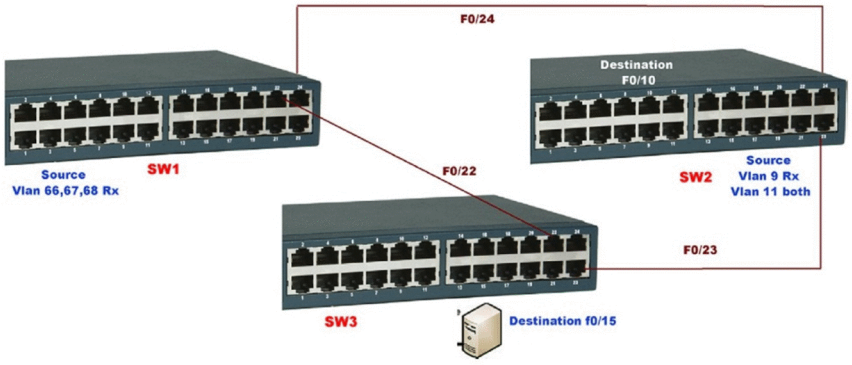
From SW2, all traffic received on VLAN 9

From SW2, all traffic sent and received on VLAN 11



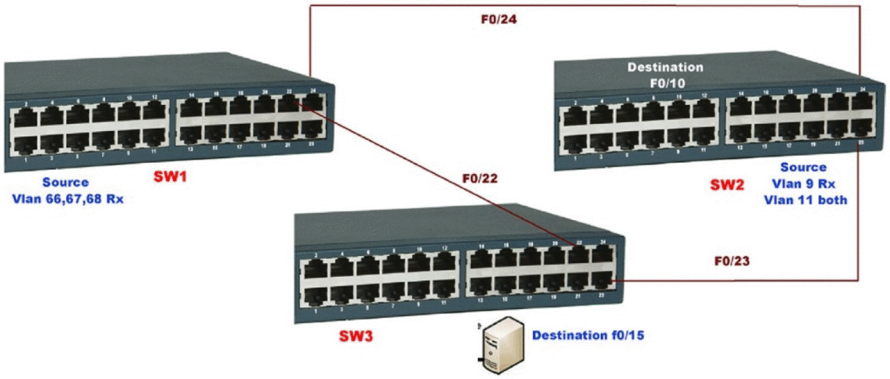
SW1(config)# **vlan 199**
SW1(config-vlan)# **remote span**
SW1(config-vlan)# **exit**

SW1(config)# **monitor session 1 source vlan 66 – 68 rx**
SW1(config)# **monitor session 1 destination remote vlan 199**



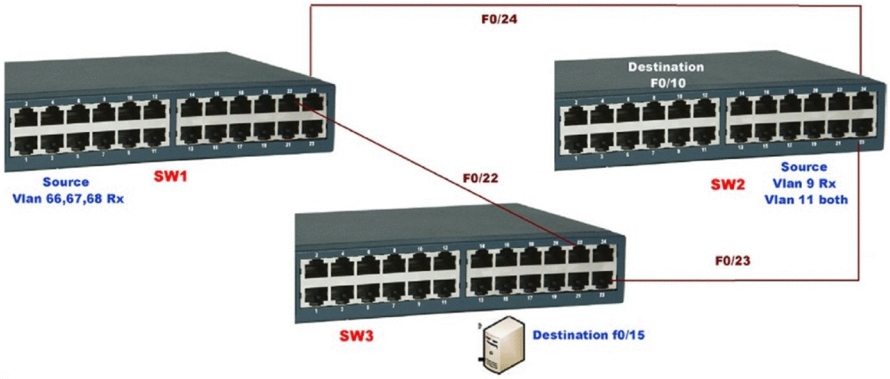
SW2(config)# **vlan 199**
SW2(config-vlan)# **remote span**
SW2(config-vlan)# **exit**

SW2(config)# **monitor session 1 source vlan 9 rx**
SW2(config)# **monitor session 1 source vlan 11**
SW2(config)# **monitor session 1 destination remote vlan 199**



SW3 (config)# **vlan 199**
SW3 (config-vlan)# **remote span**
SW3 (config-vlan)# **exit**

SW3(config)# **monitor session 3 source remote vlan 199**
SW3(config)# **monitor session 3 destination interface fa0/15**



RSPAN

To Verify

#show monitor session

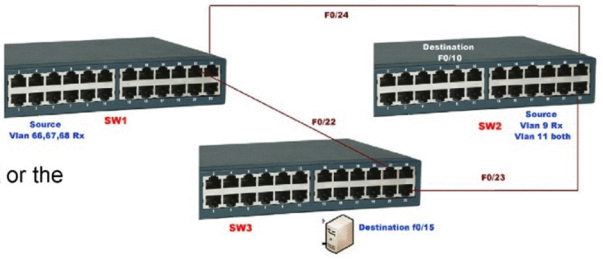
NOTE :

- RSPAN VLAN should be allowed in ALL trunks between the involved switches
- If you have enabled "pruning" in your network, remove the RSPAN VLAN from the pruning, with the command: "**switchport trunk pruning vlan remove <RSPAN VLAN ID>"** under the interface configure as trunk.

Restrictions & Conditions

source port can be any type of port

- routed port
- physical switch port
- Access port
- trunk port
- EtherChannel (either one physical port or the entire port-channel interface)
- Source VLAN

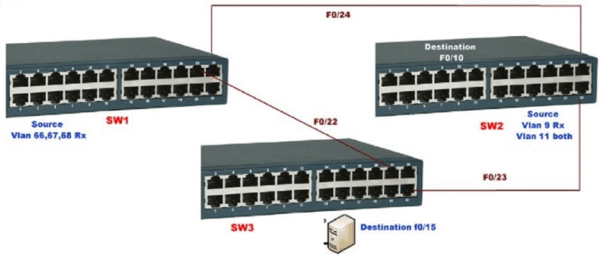


Destination ports in SPAN, RSPAN, and ERSPAN have multiple restrictions.

- its original configuration is overwritten. (the original configuration on that port is restored once remove SPAN).
- the port is removed from any EtherChannel bundle if it were part of one.
- If it were a routed port, the SPAN destination configuration overrides the routed port configuration.
- Destination ports do not support port security, 802.1x authentication, or private VLANs.
- Destination ports do not support any Layer 2 protocols, including CDP, Spanning Tree, VTP, DTP, and so on.

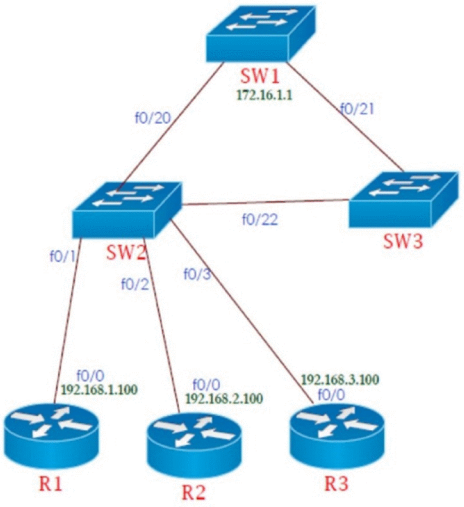
Restrictions & Conditions (Contd)

- Source can be either one or more ports or a VLAN, but not a mix of these.
- Up to 64 SPAN destination ports can be configured on a switch.
- Switched or routed ports can be configured as SPAN source ports or SPAN destination ports.
- Be careful to avoid overloading the SPAN destination port.
- A SPAN destination port cannot be a source port, and a source port cannot be a destination port.
- Only one SPAN/RSPAN/ERSPAN session can send traffic to a single destination port.
- SPAN destination port passes only SPAN-related traffic



Cisco Discovery protocol

- proprietary protocol developed by Cisco Systems.
- It is used to share information about other directly connected Cisco equipment, such as the connected ports ,operating system version and IP address.
- By default, CDP announcements are sent every 60 seconds on interfaces
- From a troubleshooting perspective, CDP can be used to either confirm or fix the documentation shown in a network diagram, or even discover the devices and interfaces used in a network.
- The show cdp neighbor command delivers information about directly connected devices.



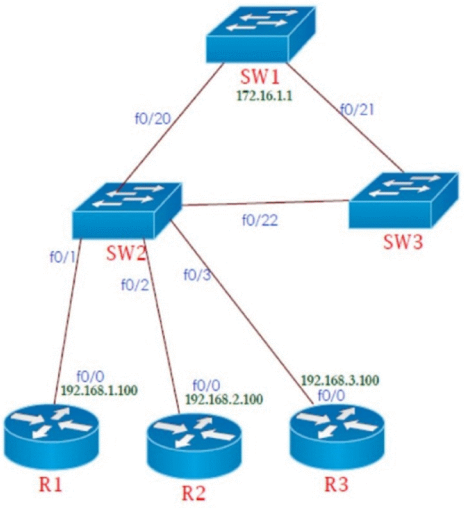
The show cdp neighbor command delivers information about directly connected devices.

#sh cdp neighbors

- Device ID
- Local Interface
- Holdtime
- Capability
- Platform
- Port ID

 # sh cdp neighbors detail

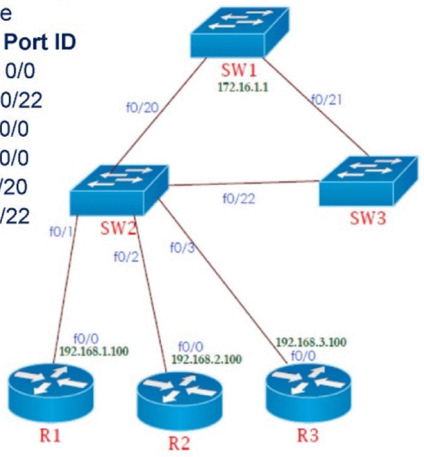
 # sh cdp interface



SW-2#sh cdp neighbors

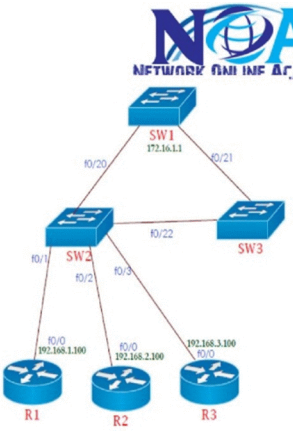
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
R-1	Fas 0/1	134	R	C2600	Fas 0/0
Switch	Fas 0/22	115	S	2950	Fas 0/22
R-2	Fas 0/2	138	R	C1841	Fas 0/0
R-3	Fas 0/3	160	R	C2800	Fas 0/0
SW-1	Fas 0/20	168		3560	Fas 0/20
SW3	Fas 0/22	175	S	2950	Fas 0/22



SW-2#sh cdp neighbors detail

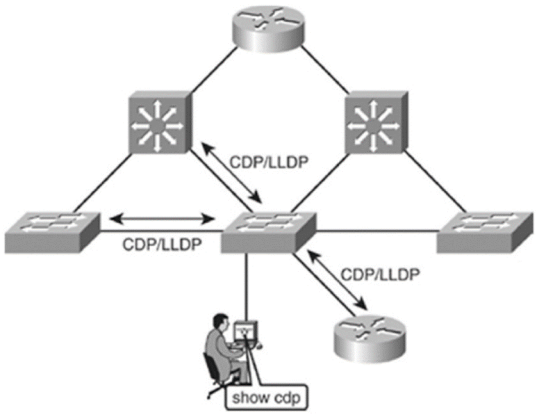
Device ID: R-1
Entry address(es):
IP address : 192.168.1.100
Platform: cisco C2600, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0
Holdtime: 125
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
advertisement version: 2
Duplex: full



Device ID: Switch
Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: FastEthernet0/22, Port ID (outgoing port): FastEthernet0/22
Holdtime: 46
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
advertisement version: 2
Duplex: full

Link Layer Discovery Protocol (LLDP).

- IEEE 802.1AB Standard (Same as CDP)
- network devices to advertise information about themselves to other devices on the network.
- This protocol can advertise details such as configuration information, device capabilities, and device identity.
  1. Port description
  2. System name
  3. System description
  4. System capabilities
  5. Management address.



LLDP Configuration

This example shows how to globally enable LLDP.

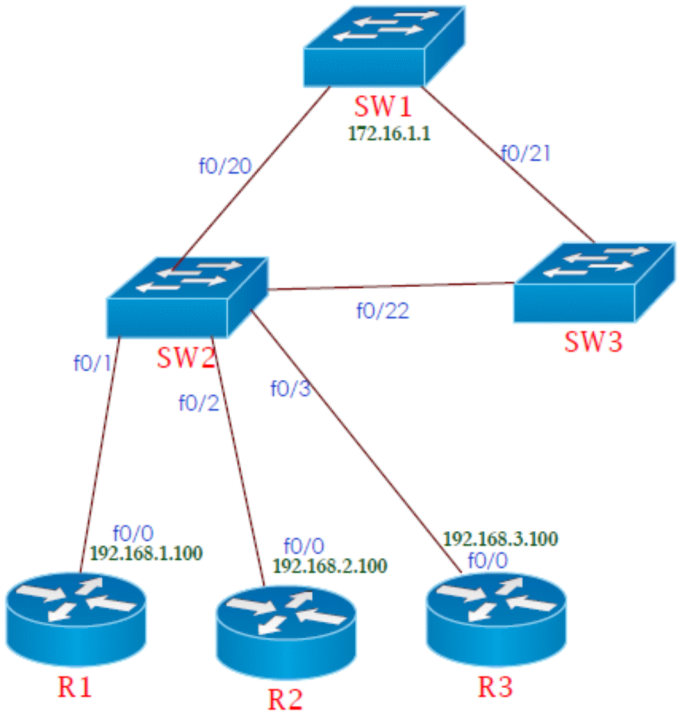
```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end
```

This example shows how to enable LLDP on an interface.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
```

```
switch# show lldp neighbor
        Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
        Device ID Local Intf    Hold-time Capability    Port ID
        c2960-8   Fa0/8         120       B             Fa0/8
```

LAB: VERIFY CDP



TASK: Confgure on R1, R2, R3, SW1 using IP address as per the Diagram.

R-1(config) #int f0/0
R-1(config-if)#ip address 192.168.1.100 255.255.255.0
R-1(config-if)#no shutdown
R-1(config-if)#exit

R-2(config)#int f0/0
R-2(config-if)#ip address 192.168.2.100 255.255.255.0
R-2(config-if)#no sh
R-2(config-if)#exit

R-3(config)#int f0/0
R-3(config-if)#ip address 192.168.3.100 255.255.255.0
R-3(config-if)#no shutdown
R-3(config-if)#exit

SW-1(config)#int vlan 1
SW-1(config-if)#ip address 172.16.1.1 255.255.255.0
SW-1(config-if)#no shutdown
SW-1(config-if)#exit

SW-2#sh cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
R-1	Fas 0/1	134	R	C2600	Fas 0/0
Switch	Fas 0/22	115	S	2950	Fas 0/22
R-2	Fas 0/2	138	R	C1841	Fas 0/0
R-3	Fas 0/3	160	R	C2800	Fas 0/0
SW-1	Fas 0/20	168		3560	Fas 0/20
SW3	Fas 0/22	175	S	2950	Fas 0/22

SW-2#sh cdp

Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled

SW-2#sh cdp interface

FastEthernet0/1 is up, line protocol is up
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/2 is up, line protocol is up
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/3 is up, line protocol is up
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/4 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/5 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/6 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/7 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/8 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/9 is down, line protocol is down
Sending CDP packets every 60 seconds

Holdtime is 180 seconds
FastEthernet0/10 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/11 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/12 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/13 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/14 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/15 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/16 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/17 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/18 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/19 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/20 is up, line protocol is up
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/21 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/22 is up, line protocol is up
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/23 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/24 is down, line protocol is down

Sending CDP packets every 60 seconds
Holdtime is 180 seconds
GigabitEthernet1/1 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
GigabitEthernet1/2 is down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

SW-2#sh cdp neighbors detail
Device ID: R-1
Entry address(es):
IP address : 192.168.1.100
Platform: cisco C2600, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0
Holdtime: 125
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
advertisement version: 2
Duplex: full

Device ID: Switch
Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: FastEthernet0/22, Port ID (outgoing port): FastEthernet0/22
Holdtime: 46
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
advertisement version: 2
Duplex: full

Device ID: R-2
Entry address(es):
IP address : 192.168.2.100
Platform: cisco C1841, Capabilities: Router
Interface: FastEthernet0/2, Port ID (outgoing port): FastEthernet0/0
Holdtime: 129

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
advertisement version: 2
Duplex: full

Device ID: R-3
Entry address(es):
IP address : 192.168.3.100
Platform: cisco C2800, Capabilities: Router
Interface: FastEthernet0/3, Port ID (outgoing port): FastEthernet0/0
Holdtime: 150
Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
advertisement version: 2
Duplex: full

Device ID: SW-1
Entry address(es):
Platform: cisco 3560, Capabilities: Router
Interface: FastEthernet0/20, Port ID (outgoing port): FastEthernet0/20
Holdtime: 159
Version :
Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 05-Jul-07 22:22 by pt_team
advertisement version: 2
Duplex: full

Device ID: SW3
Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: FastEthernet0/22, Port ID (outgoing port): FastEthernet0/22
Holdtime: 166
Version :
Cisco Internetwork Operating System Software

IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
advertisement version: 2
Duplex: full

TASK: configure SW2 to Disable CDP

SW-2(config)#no cdp run
SW-2#sh cdp
% CDP is not enabled

TASK: configure SW2 toEnable CDP

SW-2(config)#cdp run
SW-2(config)#end
SW-2#sh cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled

SW-2(config)#int f0/20
SW-2(config-if)#no cdp enable

SW-2#sh cdp interface f0/20

SW-2#sh cdp interface f0/1
FastEthernet0/1 is up, line protocol is up
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

SW-2#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

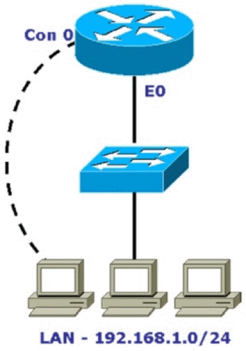
Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
R-1	Fas 0/1	136	R	C2600	Fas 0/0
R-2	Fas 0/2	140	R	C1841	Fas 0/0
R-3	Fas 0/3	161	R	C2800	Fas 0/0
SW3	Fas 0/22	177	S	2950	Fas 0/22

IOS Device Access Security

AAA, Privilege levels,

Assigning Passwords

- Console
- Auxiliary
- VTY line (telnet)



Access Port Passwords

R1(config)# enable secret cisco

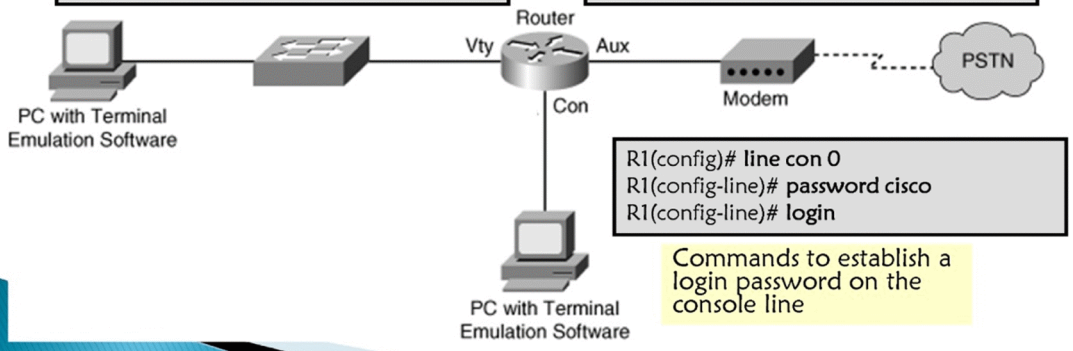
Command to restrict access to privileged EXEC mode

Commands to establish a login password on incoming Telnet sessions

R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login

Commands to establish a login password for dial-up modem connections

R1(config)# line aux 0
R1(config-line)# password cisco
R1(config-line)# login



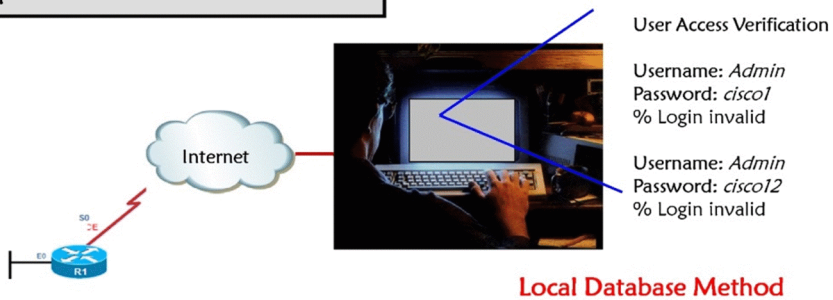
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login

Commands to establish a login password on the console line

Authentication – Local Database

- Creates individual user account/password on each device
- Provides accountability
- User accounts must be configured locally on each device

R1(config)# username Admin secret noa123
R1(config)# line vty 0 4
R1(config-line)# login local



User Access Verification

Username: *Admin*
Password: *cisco1*
% Login invalid

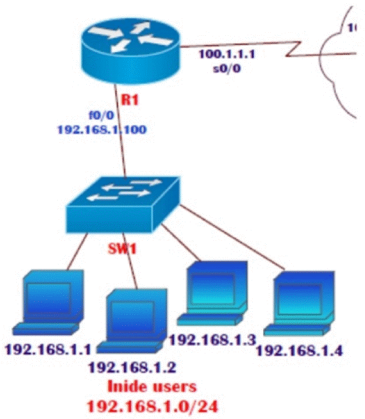
Username: *Admin*
Password: *cisco12*
% Login invalid

Local Database Method

Authentication – Local Database (contd)

router(config)#**username sikandar password noa123**

router(config)#**line vty 0 4**
router(config-line)#**login local**
router(config-line)#**exit**



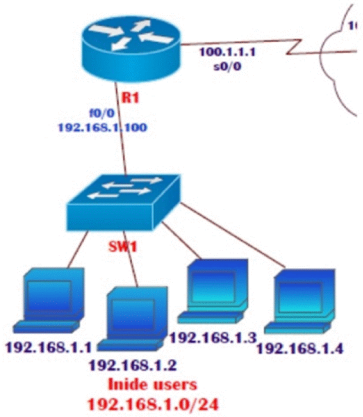
Router#**telnet 192.168.1.100**
Trying 10.1.1.1 ... Open User Access Verification

Username: **Sikandar**
password:

Authentication – Local Database (contd)

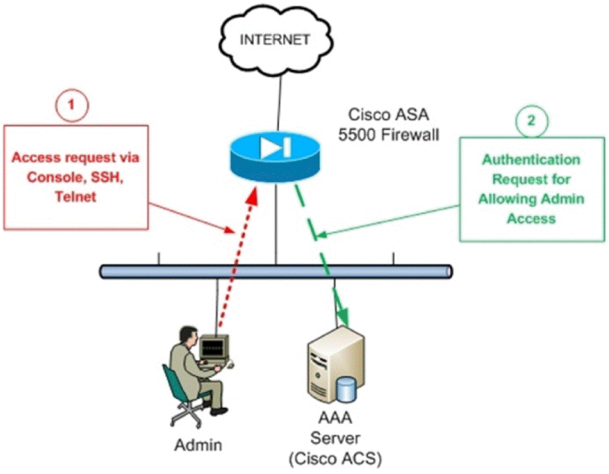
Drawbacks of Local user Authentication

- Username & passwords are stored locally
- No centralized control
- More Administrative task
- Not scalable



Using External Server Based Authentication

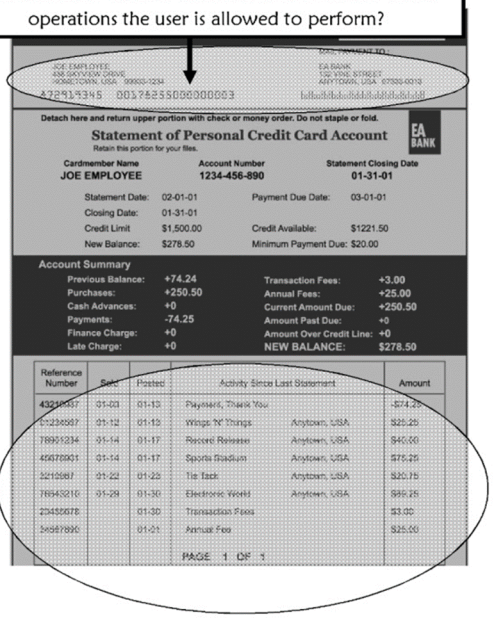
- Username & passwords are stored in remote Server.
- Allows centralized Authentication.
- Reduces Administrative Task
- Scalable.



External Authentication using AAA

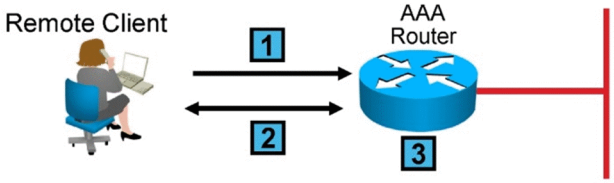
Authentication
Who are you?

Authorization
which resources the user is allowed to access and which operations the user is allowed to perform?



Accounting
What did you spend it on?

Self-Contained AAA Authentication



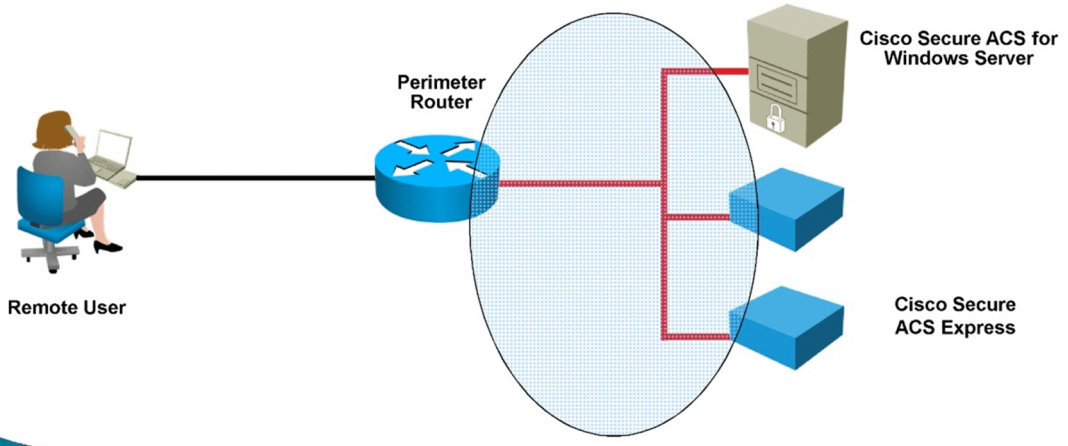
Self-Contained AAA

1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is authorized to access the network based on information in the local database.

- Used for small networks
- Stores usernames and passwords locally in the Cisco router

Server-Based AAA Authentication

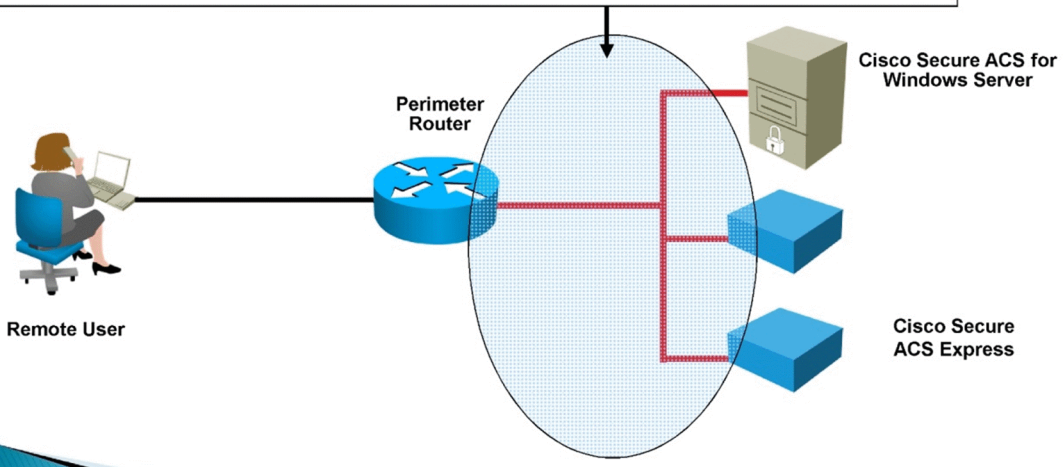
- Both **RADIUS** and **TACACS+** are client/server AAA protocols.
- Authenticate a username/password combination,
- Determine if a user is allowed to connect to the client.



Overview of TACACS+ and RADIUS

TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.

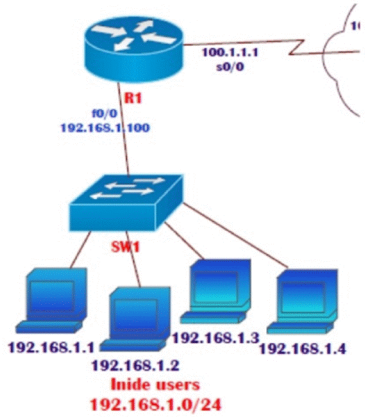
Terminal Access Controller Access Control System
Remote authentication dial in user service



Local AAA Authentication Configuration

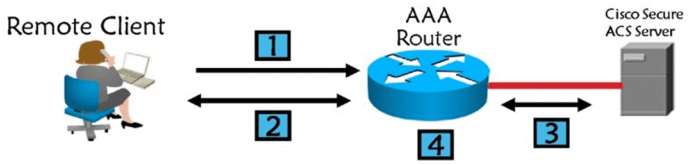
R-1(config)#aaa new-model
R-1(config)#username sikandar password noa123
R-1(config)#aaa authentication login default local

R-1(config)#line console 0 / vty 0 4
R-1(config-line)#login authentication default
R-1(config-line)#exit



Server-Based AAA Authentication

- Centrally validate users wishing to gain access to a resource such as a router
- Uses an external database server
  - Cisco Secure Access Control Server (ACS) for Windows Server
  - Cisco Secure ACS Solution Engine
  - Cisco Secure ACS Express
- More appropriate if there are multiple routers



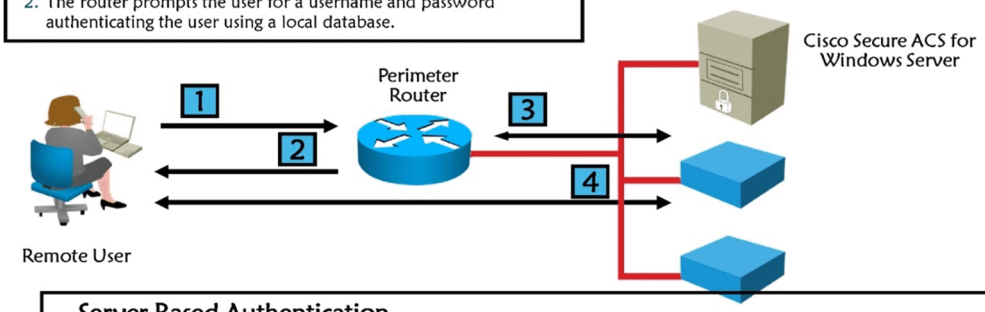
Server-Based AAA

1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is authorized to access the network based on information on the remote AAA Server.

Local Versus Server-Based Authentication

Local Authentication

1. The user establishes a connection with the router.
2. The router prompts the user for a username and password authenticating the user using a local database.

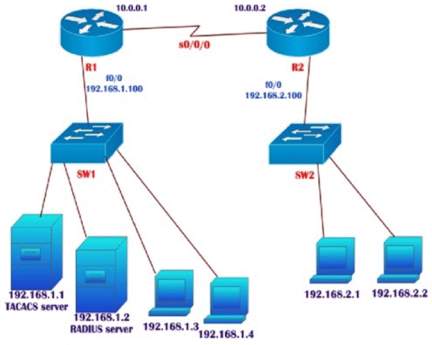


Server-Based Authentication

1. The user establishes a connection with the router.
2. The router prompts the user for a username and password.
3. The router passes the username and password to the Cisco Secure ACS (server or engine).
4. The Cisco Secure ACS authenticates the user. The user is authorized to access the router (administrative access) or the network based on information found in the Cisco Secure ACS database.

AAA Authentication using TACACS+

```
R-1(config)#no aaa new-model

R-1(config)#username sikandar password noa123
R-1(config)#tacacs-server host 192.168.1.1
R-1(config)#tacacs-server key sikandar123

R-1(config)#aaa new-model
R-1(config)#aaa authentication login default group tacacs+ local

R-1(config)#line con 0
R-1(config-line)#login authentication default
R-1(config-line)#exit
R-1(config)#end
```



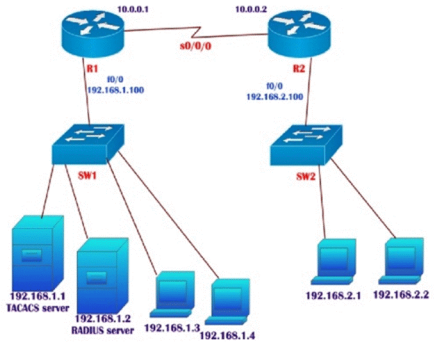
AAA Authentication using RADIUS Server

R-1(config)#no aaa new-model

R-1(config)#username sikandar password noa123
R-1(config)#radius-server host 192.168.1.1
R-1(config)#tradius-server key sikandar123

R-1(config)#aaa new-model
R-1(config)#aaa authentication login default group Radius local

R-1(config)#line con 0
R-1(config-line)#login authentication default
R-1(config-line)#exit
R-1(config)#end



Password Security

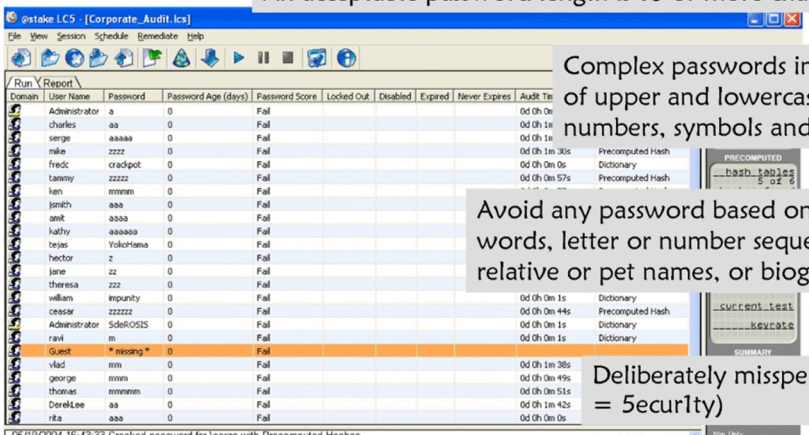
To increase the security of passwords, use additional configuration parameters:

- Minimum password lengths should be enforced
- Unattended connections should be disabled
- All passwords in the configuration file should be encrypted

```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config
line con 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
line aux 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
```

Passwords

An acceptable password length is 10 or more characters



Complex passwords include a mix of upper and lowercase letters, numbers, symbols and spaces

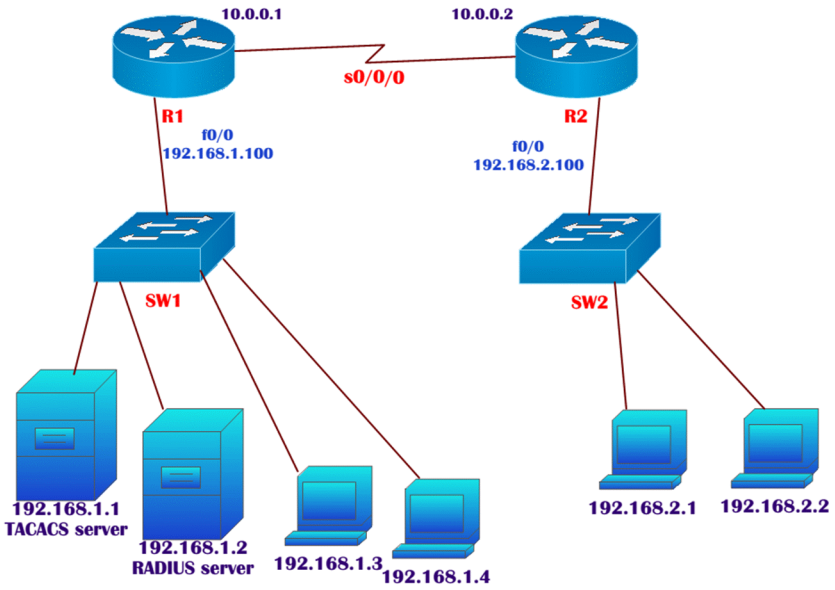
Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, or biographical information

Deliberately misspell a password (Security = 5ecur1ty)

Change passwords often

Do not write passwords down and leave them in obvious places

LAB: AAA Authentication using External servers



TASK:

- Configure Basic IP addressing as per the Diagram and Ensure that there is reachability between Them

Router(config)#hostname R-1
R-1(config)#int f0/0
R-1(config-if)#ip address 192.168.1.100 255.255.255.0
R-1(config-if)#no shutdown
R-1(config-if)#exit

R-1(config)#int s0/0/0
R-1(config-if)#ip address 10.0.0.1 255.0.0.0
R-1(config-if)#no shutdown
R-1(config-if)#clock rate 64000
R-1(config-if)#end

R2

R-2(config)#int f0/0
R-2(config-if)#ip address 192.168.2.100 255.255.255.0
R-2(config-if)#no shutdown
R-2(config-if)#exit

R-2(config)#interface serial 0/0/0
R-2(config-if)#ip address 10.0.0.2 255.0.0.0
R-2(config-if)#no sh
R-2(config-if)#clock rate 64000
R-2(config-if)#end

R-2#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/12/37 ms

R-2#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/6 ms

TASK: Configure Local AAA Authentication for Console Access on R1

R-1(config)#username sikandar password cisco123
R-1(config)#aaa new-model
R-1(config)#aaa authentication ?
enable Set authentication lists for enable.
login Set authentication lists for logins.
ppp Set authentication lists for ppp.

R-1(config)#aaa authentication login default ?
enable Use enable password for authentication.
group Use Server-group.
local Use local username authentication.
none NO authentication.

R-1(config)#aaa authentication login default local

R-1(config)#line console 0
R-1(config-line)#login authentication default
R-1(config-line)#exit

R-1(config)#end
R-1#exit
User Access Verification
Username: sikandar
Password:
R-1>
R-1>enable

R-1#exit

TASK:

- Configure Local AAA Authentication for VTY Lines on R1

```
R-1(config)#line vty 0 15
R-1(config-line)#login authentication default
R-1(config-line) #exit

R-1(config) #enable  secret cisco
```

Verify the AAA authentication method.

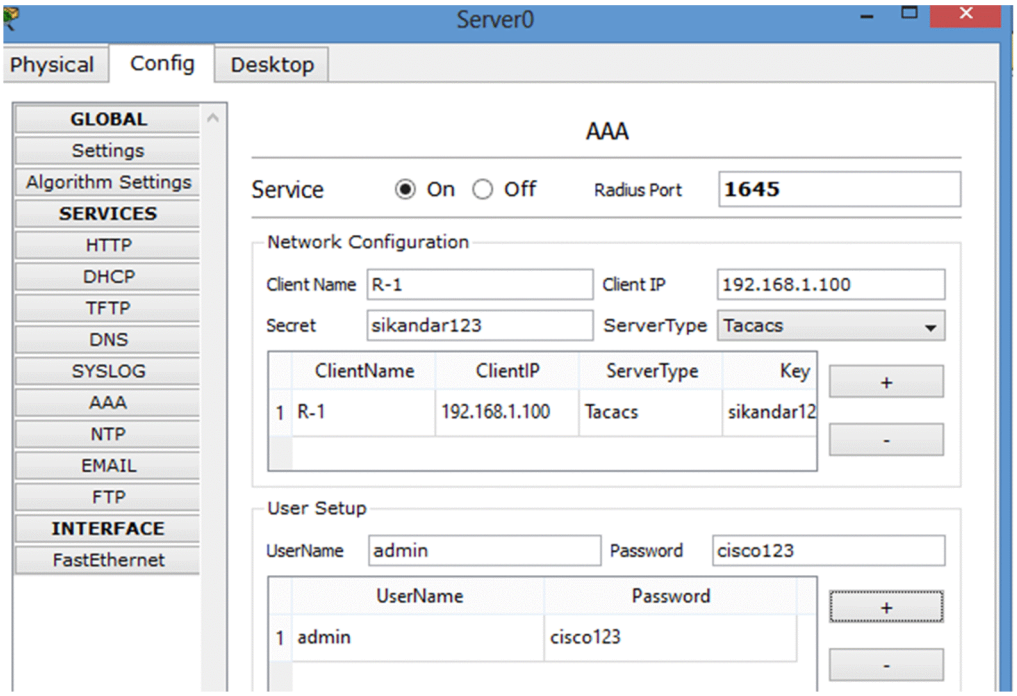
Verify the Telnet configuration. From the command prompt of PC (192.168.1.3) Telnet to R1.

On PC

```
PC>telnet 192.168.1.100
Trying 192.168.1.100 ...Open
User Access Verification
Username: sikandar
Password:
R-1>enable
Password:
R-1#exit
[Connection to 192.168.1.100 closed by foreign host]
```

TASK:

- Remove th AAA configs done in the previous tasks
- Configure Server-Based AAA Authentication Using TACACS+ protocol (192.168.1.1) on R1
- Fallback to local authentication if server does not respond.




```
R-1(config)#no aaa new-model

R-1(config)#username sikandar password cisco123
R-1(config)#tacacs-server host 192.168.1.1
R-1(config)#tacacs-server key sikandar123

R-1(config)#aaa new-model
R-1(config)#aaa authentication login default ?
        enable  Use enable password for authentication.
        group   Use Server-group.
        local   Use local username authentication.
        none    NO authentication.

R-1(config)#aaa authentication login default group tacacs+ ?
        enable  Use enable password for authentication.
        group   Use Server-group.
        local   Use local username authentication.
        none    NO authentication.
        <cr>
R-1(config)#aaa authentication login default group tacacs+ local

R-1(config)#line con 0
R-1(config-line)#login authentication default
R-1(config-line)#exit
R-1(config)#end
R-1#exit
```

R-1 con0 is now available

Press RETURN to get started.

User Access Verification
Username: admin
Password:

R-1>
R-1>enable
Password:
R-1#

TASK:

- Configure AAA Authentication for VTY Lines on R1 using TACACS server.

R-1(config)#line vty 0 4
R-1(config-line)#login authentication default
R-1(config-line)#exit

PC>ipconfig
IP Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>telnet 192.168.1.100
Trying 192.168.1.100 ...Open
User Access Verification
Username: admin
Password:

R-1>enable
Password:
R-1#
R-1#sh users

	Line	User	Host(s)	Idle	Location
	0 con 0	admin	idle	00:00:44	
*	67 vty 0		idle	00:00:00	192.168.1.3

TASK

- Configure R2 to use AAA authentication using external AAA server (192.168.1.2) RADIUS protocol
- Fallback to local authentication if server does not respond.
- Using EIGRP as routing Protocol to provide connectivity between the two networks

Username: admin

Password:

R-1>enable
Password:

R-1#conf terminal
R-1(config)#router eigrp 100
R-1(config-router)#network 10.0.0.0
R-1(config-router)#network 192.168.1.0
R-1(config-router)#exit

R-2(config)#router eigrp 100
R-2(config-router)#network 10.0.0.0
R-2(config-router)#network 192.168.2.0
R-2(config-router)#end

R-2#sh ip eigrp neighbors

IP-EIGRP neighbors for process 100

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	10.0.0.1	Se0/0/0	11	00:00:14	40	1000	0	3

R-2#sh ip route eigrp

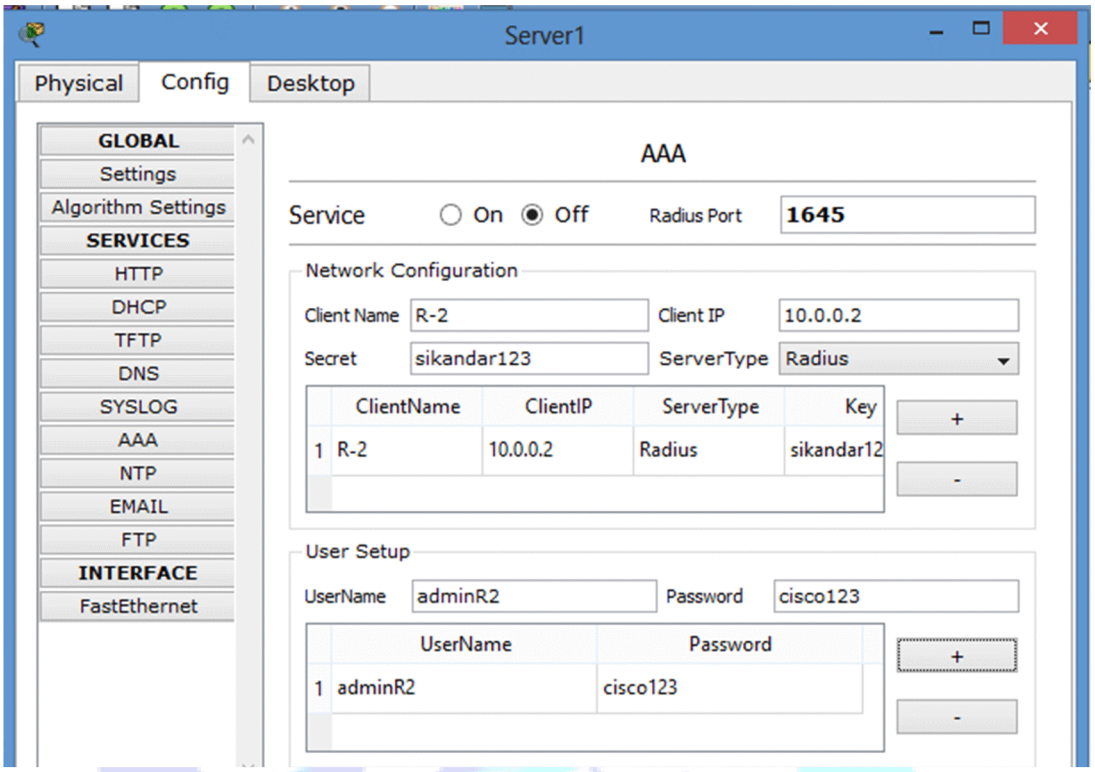
D 192.168.1.0/24 [90/2172416] via 10.0.0.1, 00:00:16, Serial0/0/0

R-2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/13/16 ms

R-2#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/10/16 ms



R-2(config)#username sikandar password cisco123

R-2(config)#radius-server host 192.168.1.2
R-2(config)#radius-server key sikandar123

R-2(config)#aaa new-model

R-2(config)#aaa authentication login default group radius ?
enable Use enable password for authentication.
group Use Server-group.
local Use local username authentication.
none NO authentication.
<cr>

R-2(config)#aaa authentication login default group radius local

R-2(config)#line con 0
R-2(config-line)#login authentication default
R-2(config-line)#exit
R-2(config)#exit
R-2#exit

Press RETURN to get started.

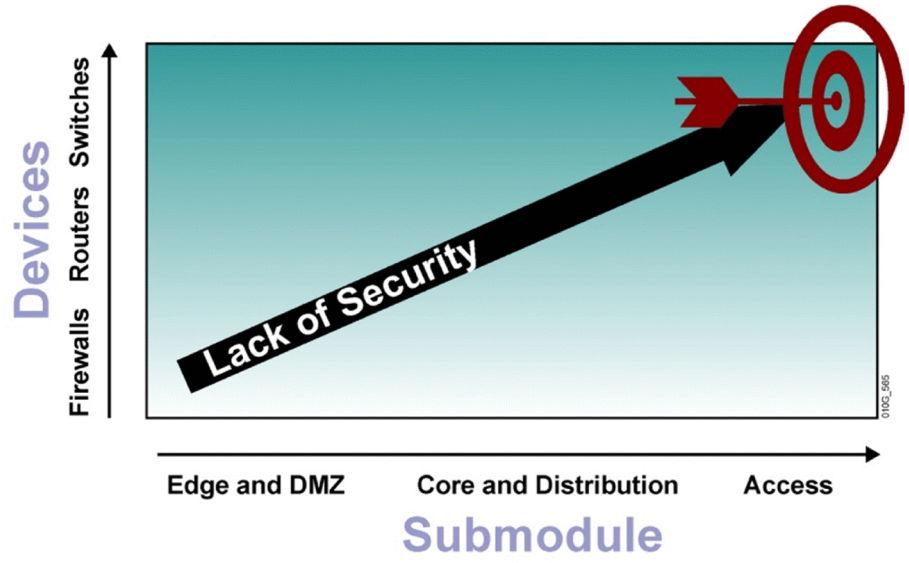
```
User Access Verification
Username: adminR2
Password:

R-2>enable
Password:

R-2#sh users
    Line       User       Host(s)              Idle       Location
  * 0 con 0    adminR2    idle                 00:00:00
  Interface    User               Mode         Idle     Peer Address
```

TASK: Configure AAA Authentication for VTY Lines on R2 using RADIUS server.

```
R-2(config)#line vty 0 4
R-2(config-line)#login authentication default
R-2(config-line)#exit
R-2(config)#

PC>ipconfig
   IP Address.....: 192.168.2.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.2.100

PC>telnet 192.168.2.100
   Trying 192.168.2.100 ...Open
   User Access Verification
   Username: adminR2
   Password:

R-2>enable
Password:
R-2#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0     adminR2    idle                 00:00:36
* 67 vty 0                idle                 00:00:00 192.168.2.1
  Interface    User               Mode         Idle     Peer Address
```

Understanding Switch Security Issues

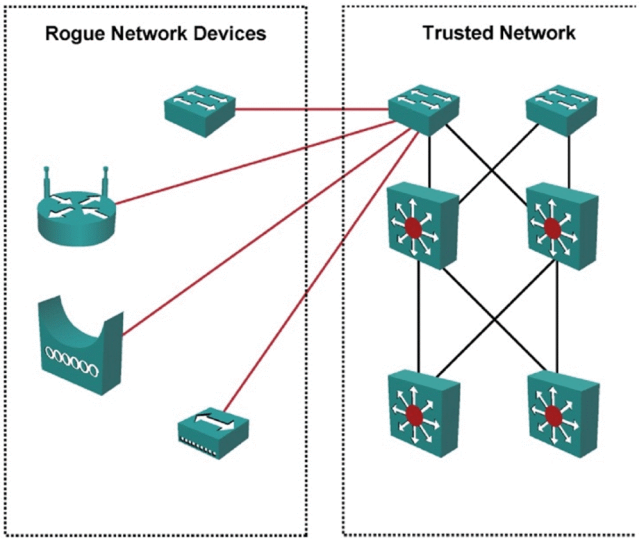
Overview of Switch Security



Rogue Access Points

Rogue network devices
- Wireless hubs
- Wireless routers
- Access switches
- Hubs

These devices are typically connected at access level switches.

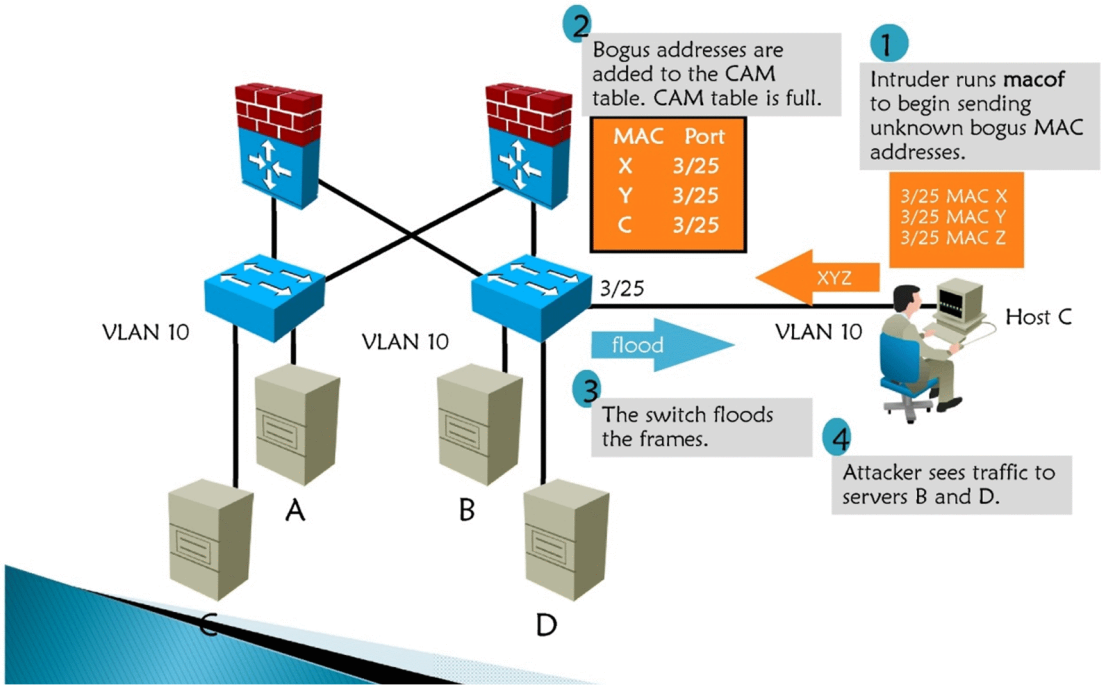


Switch Attack Categories & solution

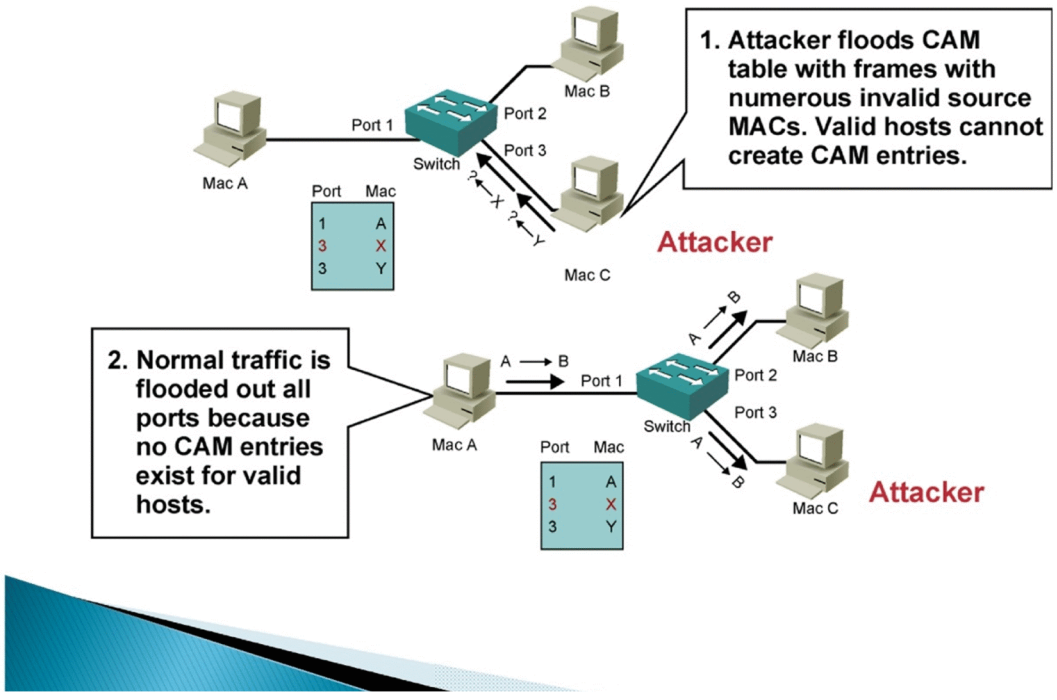
Layer 2 Attacks :
- MAC table overflow attacks
- VLAN attacks
- Spoofing attacks (Mac, IP , ARP, DHCP)

Switch Security:
- Port-security
- DHCP Snooping
- IP source Guard
- Dynamic ARP Inspection
- Storm Control

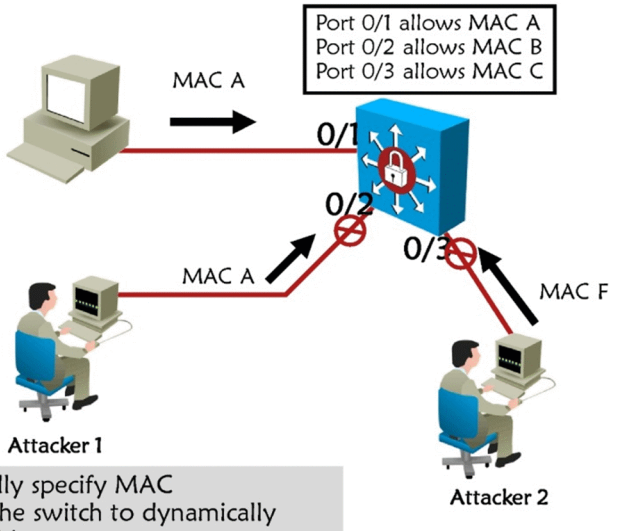
MAC Address Table Overflow Attack



MAC Flooding Attack



Port Security Overview



Allows an administrator to statically specify MAC Addresses for a port or to permit the switch to dynamically learn a limited number of MAC addresses

Port Security Configuration

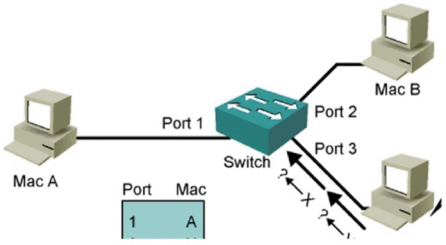
(config)# interface f0/1

(config-if)# switchport mode access

(config-if)# switchport port-security

(config-if)# switchport port-security maximum *value*

(config-if)# switchport port-security violation {protect | restrict | shutdown}



Note:

- Port-security works only on ports configured as static access or static trunks (does not work on dynamic ports)
- the default "shutdown" action

Port-Security Violation Parameters

(config-if)# switchport port-security violation {protect |restrict | shutdown}

Shutdown

- port immediately is put into the Err-disable state

Protect

- The port is allowed to stay up, as in the restrict mode.
- Reaches its MAC address limit, the port stops learning MAC addresses
- Although packets from violating addresses are dropped, no record of the violation is kept.

Restrict

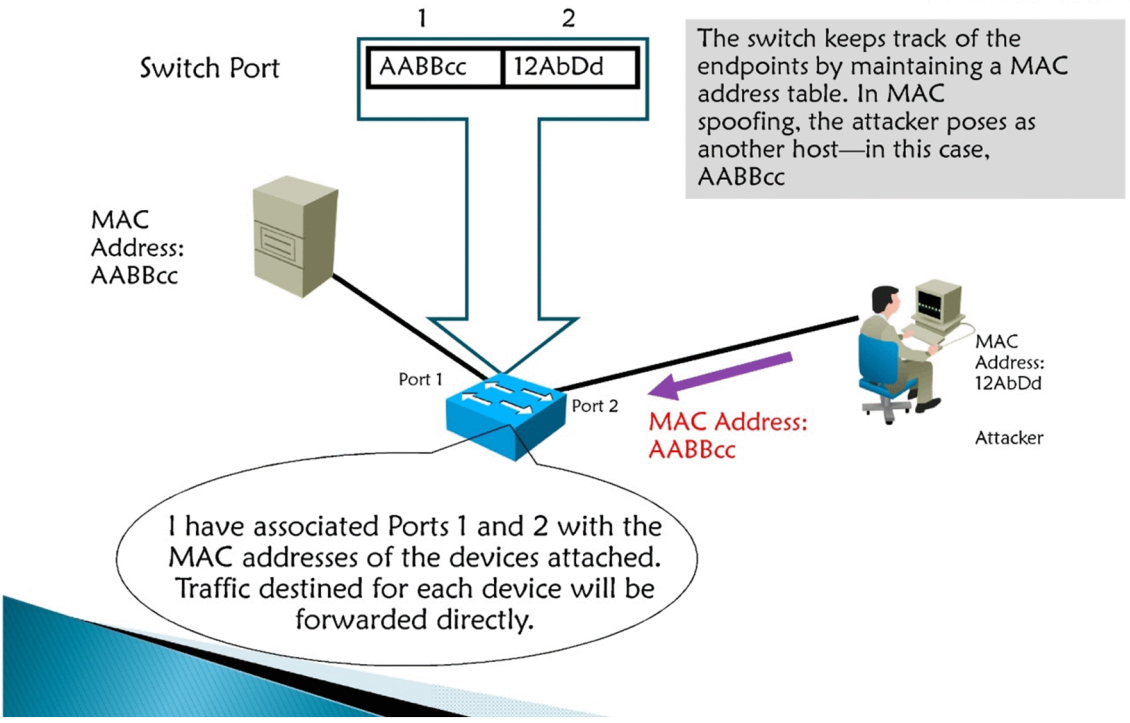
- The port is allowed to stay up, but all packets from violating MAC addresses are dropped.
- The switch keeps a running count of the number of violating packets and can send an SNMP trap and a syslog message as an alert of the violation.

Verifying Port Security

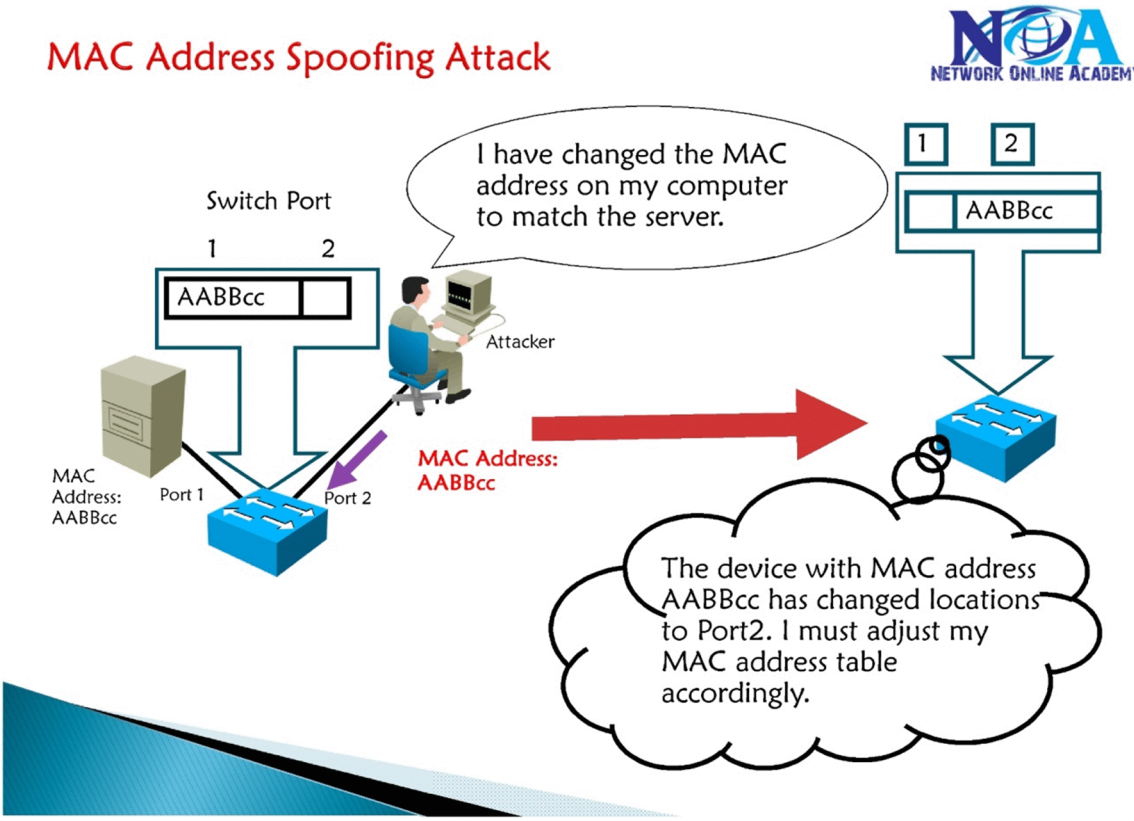
Displays MAC address table security information

```
Switch#show port-security address
            Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
1    0001.0001.0001    SecureDynamic       Fa5/1      15 (I)
1    0001.0001.0002    SecureDynamic       Fa5/1      15 (I)
1    0001.0001.1111    SecureConfigured    Fa5/1      16 (I)
1    0001.0001.1112    SecureConfigured    Fa5/1      -
1    0001.0001.1113    SecureConfigured    Fa5/1      -
1    0005.0005.0001    SecureConfigured    Fa5/5      23
1    0005.0005.0002    SecureConfigured    Fa5/5      23
1    0005.0005.0003    SecureConfigured    Fa5/5      23
1    0011.0011.0001    SecureConfigured    Fa5/11     25 (I)
1    0011.0011.0002    SecureConfigured    Fa5/11     25 (I)
------------------------------------------------------------------------
Total Addresses in System: 10
Max Addresses limit in System: 128
```

MAC Address Spoofing Attack

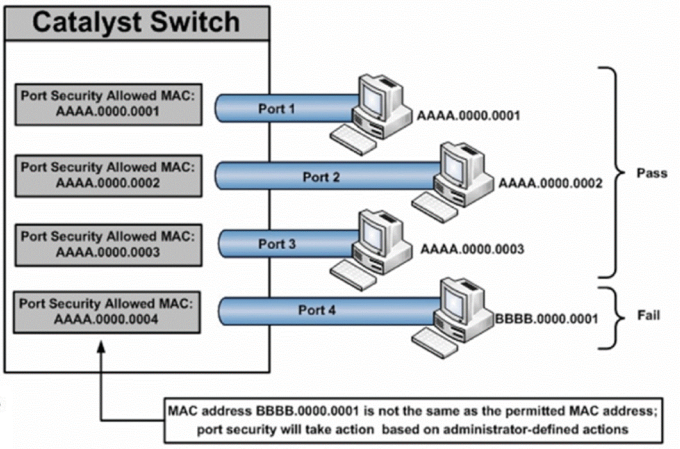


MAC Address Spoofing Attack

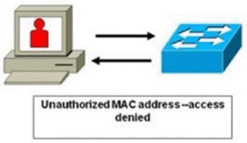


MAC Address Spoofing Attack (solution)

Binding MAC address to specific ports
Manually / Dynamically



Port security restricts port access by MAC address.



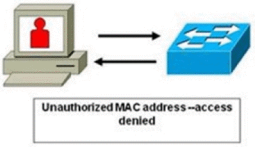
Port Security (Binding MAC addresses)

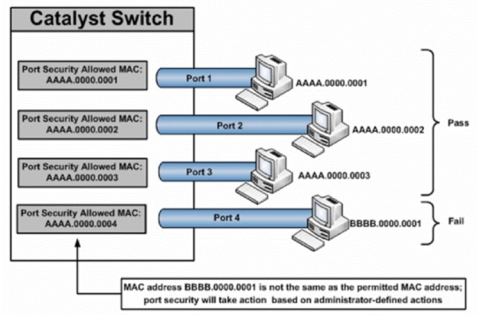
(config)# interface Fastethernet 0/10
(config-if)# switchport mode access

(config-if)# switchport port-security
(config-if)# switchport port-security maximum *value*

(config-if)# switchport port-security violation {protect | restrict | shutdown}

Port security restricts port access by MAC address.





Manual Binidng MAC addresses

(config-if)# switchport port-security mac-address *mac-address*

OR

Dynamic Binding of Learned MAC Address

(config-if)# switchport port-security mac-address sticky

View Secure MAC Addresses

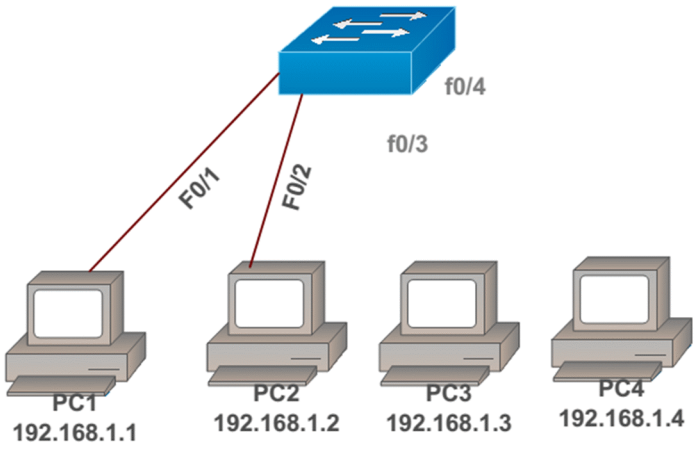
```
sw-class# show port-security address

Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports    Remaining Age
                                                          (mins)
----    -----------       ----                  -----    -------------
   1    0000.ffff.aaaa    SecureConfigured      Fa0/12       -
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Verify Port-security

```
sw-class# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
             (Count)        (Count)      (Count)
---------------------------------------------------------------------------
   Fa0/12         2             0             0          Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

```
sw-class# show port-security interface f0/12
Port Security              : Enabled
Port status                : Secure-down
Violation mode             : Shutdown
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Aging time                 : 120 mins
Aging type                 : Absolute
SecureStatic address aging : Disabled
Security Violation Count   : 0
```

LAB : PORT-SECURITY



TASK :

- Configure Port-security on f0/1 with maximum mac-address limit to 2
- also the mac-address sticky option to bind the Mac on port f0/1
- if it exceeds it has to apply the default violation rule (shutdown)

```
Switch(config)#int f0/1
Switch(config-if)#switchport port-security
    Command rejected: FastEthernet0/1 is a dynamic port.

Switch(config)# int f0/1
Switch(config-if)#  switchport mode access
Switch(config-if)#  switchport port-security
Switch(config-if)#  switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#end

Switch#sh running-config
    Building configuration...

    interface FastEthernet0/1
     switchport mode access
     switchport port-security
     switchport port-security maximum 2
    switchport port-security mac-address sticky

Switch#clear mac-address-table

Switch#sh mac-address-table
            Mac Address Table
    ------------------------------------------

    Vlan    Mac Address       Type        Ports
```

```
----    ----------      --------    -----

Switch#sh port-security
    Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)       (Count)
    ---------------------------------------------------------------------
          Fa0/1       2          0              0        Shutdown
    ---------------------------------------------------------------------
```

TASK :

- Configure F0/1 port to use port-fast to ensure that it comes to forwarding immediately.
- Connect PC(192.168.1.1) on f0/1 and generate traffic by using ping to other devices in the LAN.
- Try connecting another device and generate traffic to test Port-security violation rule.

```
Switch(config)#int f0/1
Switch(config-if)#spanning-tree portfast
Switch(config-if)#end
```

NOTE :

In order to test and verify we are using port-fast (portfast is not mandatory to configure port-security) . here we are using to speed up the access ports convergence time.

```
PC>ipconfig
    FastEthernet0 Connection:(default port)

      Link-local IPv6 Address.....: ::
      IP Address.....: 192.168.1.1
      Subnet Mask.....: 255.255.255.0
      Default Gateway.....: 192.168.1.100

PC>ping 192.168.1.2
    Pinging 192.168.1.2 with 32 bytes of data:

    Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
    Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
    Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
    Reply from 192.168.1.2: bytes=32 time=0ms TTL=128

    Ping statistics for 192.168.1.2:
        Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Switch#sh mac-address-table
```

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.974d.5308    DYNAMIC     Fa0/2
   1    0005.5e88.800b    STATIC      Fa0/1
```

Switch#sh run

```
Building configuration...

spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0005.5E88.800B
 spanning-tree portfast
```

Switch#sh port-security

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
             (Count)       (Count)       (Count)
---------------------------------------------------------------------------
      Fa0/1       2          1              0         Shutdown
---------------------------------------------------------------------------
```

Sticky will automatically bind the mac-address learned on f0/1 port.
maximum mac-address option will not allow to learn more than one mac-address as per our configuration here.

TASK :

- Remove the PC connected on f0/1 and try connecting another PC (here 192.168.1.3) and generate traffic from new PC connected.

Switch#sh running-config

```
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0005.5E88.800B
```

switchport port-security mac-address sticky 00E0.A325.1980
spanning-tree portfast

Switch#sh port-security

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	2	2	0	Shutdown

TASK :

- Connect PC4 (192.168.1.4) to f0/1 port by removing 192.168.1.3
- Verify as per the configuration the f0/1 port should go in to err-disable state.

PC>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::20C:CFFF:FEE2:3946
IP Address.....: 192.168.1.4
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 0.0.0.0

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Switch#sh ip int brief

Interface	IP-Address	OK? Method	Status	Protocol
FastEthernet0/1	unassigned	YES manual	down	down

TASK :

- Reconnect PC1 (192.168.1.1) back on f0/1 port.
- and ensure that port comes back to up state and should be reach other devices in the LAN.

Switch#sh ip int brief

Interface	IP-Address	OK? Method	Status	Protocol
FastEthernet0/1	unassigned	YES manual	down	down

```
Switch(config)#int f0/1
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
Switch(config-if)#end

Switch#sh ip int brief
    Interface              IP-Address      OK? Method Status                Protocol
    FastEthernet0/1        unassigned      YES manual up                    up

Switch#sh running-config

    interface FastEthernet0/1
     switchport mode access
     switchport port-security
     switchport port-security maximum 2
     switchport port-security mac-address sticky
     switchport port-security mac-address sticky 0005.5E88.800B
     switchport port-security mac-address sticky 00E0.A325.1980
     spanning-tree portfast

Switch#sh mac-address-table
              Mac Address Table
    -------------------------------------------

    Vlan    Mac Address       Type        Ports
    ----    -----------       --------    -----

       1    0001.974d.5308    DYNAMIC     Fa0/2
       1    0005.5e88.800b    STATIC      Fa0/1
       1    00e0.a325.1980    STATIC      Fa0/1
```

On f0/1 there is MAC biniding done with PC1 and PC2 Mac-address. if anyother device is connected on f0/1 it will put the port in to shutdown state.

TASK: Confugure the Violation rule to protect mode instead of shutdown

```
Switch(config)#int f0/1
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode

Switch(config-if)#switchport port-security violation protect
Switch(config-if)#end
```

Switch#sh running-config

```
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation protect
 switchport port-security mac-address sticky 0005.5E88.800B
 switchport port-security mac-address sticky 00E0.A325.1980
 spanning-tree portfast
!
```

To test connect PC3 to f0/1 and try generating traffic to other devices in the LAN,

Switch#sh ip int brief

```
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
```

Switch#show port-security

```
  Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)       (Count)       (Count)
  ---------------------------------------------------------------------
        Fa0/1       2           2              0          Protect
---------------------------------------------------------------------
```

PC>ipconfig

```
FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::20C:CFFF:FEE2:3946
   IP Address.....: 192.168.1.4
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 0.0.0.0
```

PC>ping 192.168.1.2

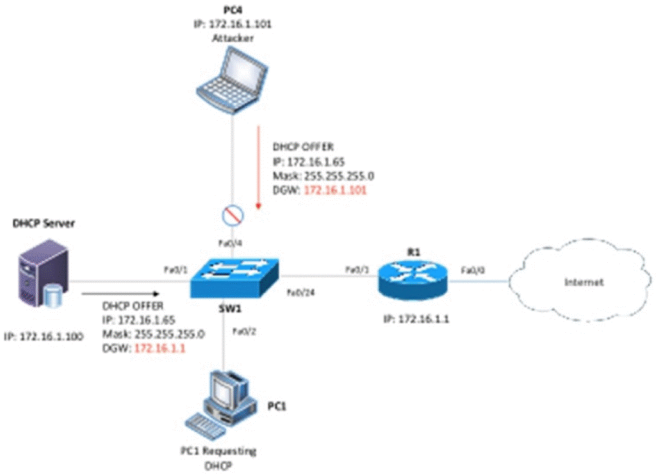
```
Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Ping statistics for 192.168.1.2:

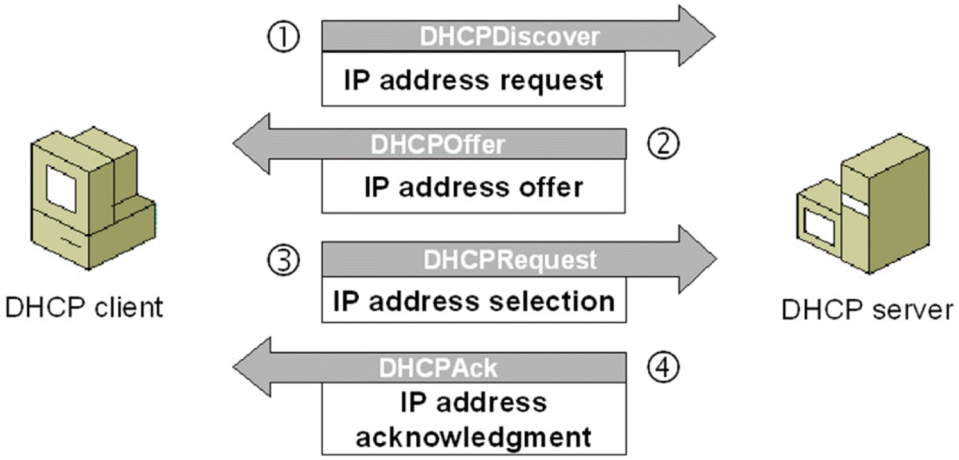
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

DHCP spoofing Attack

- Attacker activates DHCP server on VLAN.
- Attacker replies to valid client DHCP requests.
- Attacker assigns IP configuration information that establishes rogue device as client default gateway.
- Attacker establishes "man-in-the-middle" attack.

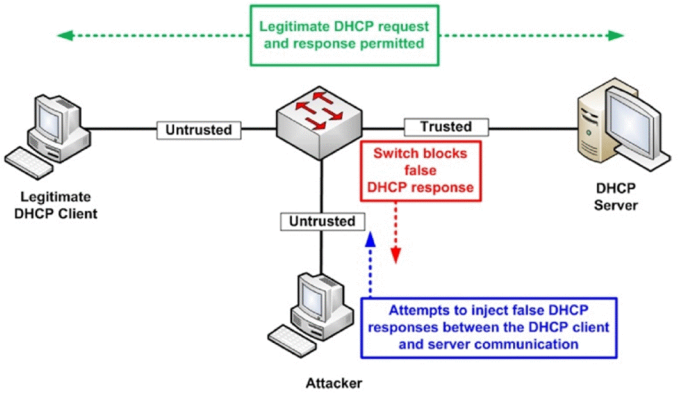


DHCP Process

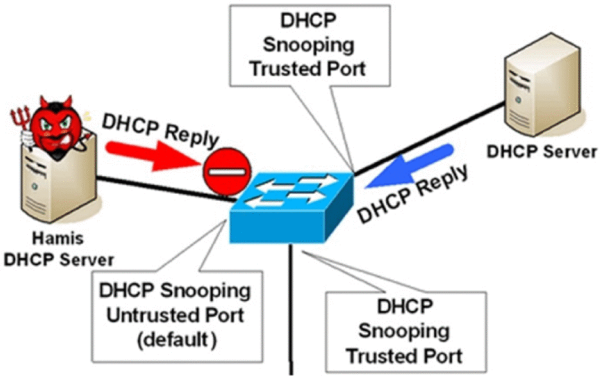


DHCP Snooping

- DHCP snooping allows the configuration of ports as trusted or untrusted.
- Untrusted ports cannot process DHCP replies.
- Configure DHCP snooping on uplinks to a DHCP server.
- Do not configure DHCP snooping on client ports.



DHCP Snooping Configuration



Switch(config)# **ip dhcp snooping**
Switch(config)# **ip dhcp snooping vlan number [number]**

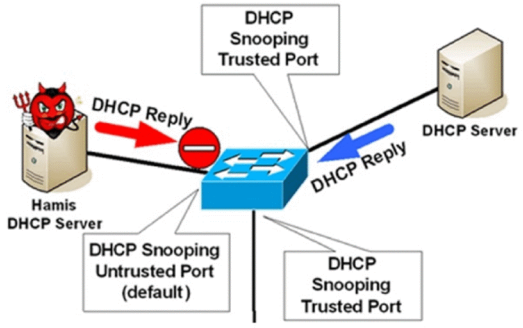
Switch(config)# **interface f0/1**
Switch(config-if)# **ip dhcp snooping trust**

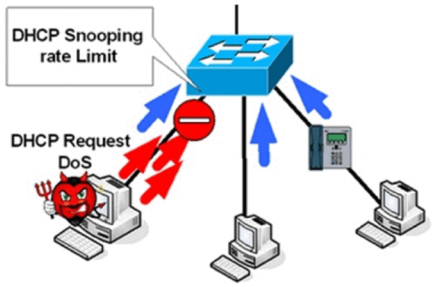
Verifying DHCP Snooping

```
Switch# show ip dhcp snooping
```

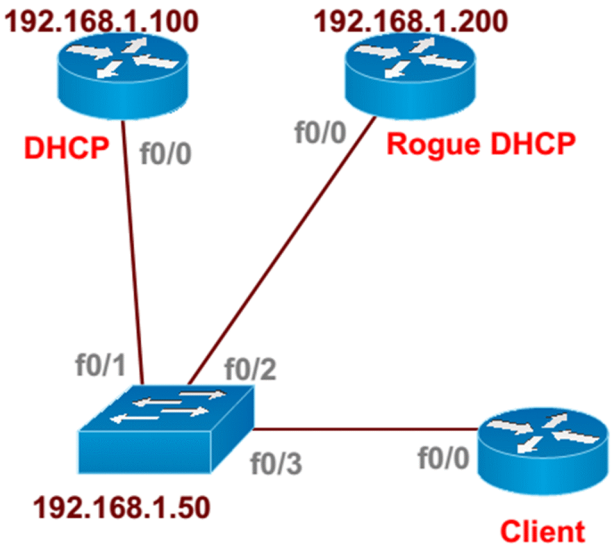
- Verifies the DHCP snooping configuration

```
Switch# show ip dhcp snooping
    Switch DHCP snooping is enabled
    DHCP Snooping is configured on the following VLANs:
        10 30-40 100 200-220
    Insertion of option 82 information is enabled.
    Interface            Trusted        Rate limit (pps)
    ---------            -------        ----------------
    FastEthernet2/1      yes            none
    FastEthernet2/2      yes            none
    FastEthernet3/1      no             20
```





LAB : DHCP Snooping :



TASK :

- Create vlan 10 and assign IP address 192.168.1.50 on vlan 10 interface.
- Connect devices as per the diagram and configure f0/1 – 4 ports in vlan 10.
- Enable portfast on these ports for faster convergence.(to test not mandatory)

```
SW1(config)#vlan 10
SW1(config-vlan)#exit

SW1(config)#int vlan 10
SW1(config-if)#ip address 192.168.1.50 255.255.255.0
SW1(config-if)#exit

SW1(config)#int range f0/1 - 4
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#spanning-tree portfast
SW1(config-if-range)#no shutdown
SW1(config-if-range)#end
```

TASK :

- Configure R1 to be DHCP server and verifty on R3 (as DHCP client) .
- use network range 192.168.1.0/24 and R1 should be default Gateway (192.168.1.100) .

```
R-1(config)#int f0/0
R-1(config-if)#ip address 192.168.1.100 255.255.255.0
R-1(config-if)#no shutdown
R-1(config-if)#exit

R-1(config)#ip dhcp pool CCIE
R-1(dhcp-config)#network 192.168.1.0 255.255.255.0
```

```
R-1(dhcp-config)#default-router 192.168.1.100
R-1(dhcp-config)#exit

R-1#sh ip dhcp pool
        Pool CCIE :
         Utilization mark (high/low)    : 100 / 0
         Subnet size (first/next)       : 0 / 0
         Total addresses                : 254
         Leased addresses               : 0
         Pending event                  : none
         1 subnet is currently in the pool :
         Current index        IP address range                  Leased addresses
         192.168.1.1          192.168.1.1      - 192.168.1.254     0


R3-DCHPClient(config)#int f0/0
R3-DCHPClient(config-if)#ip address dhcp
R3-DCHPClient(config-if)#no shutdown
R3-DCHPClient(config-if)#end

DCHPClient#sh ip int brief
        Interface              IP-Address      OK? Method Status                Protocol
        FastEthernet0/0        192.168.1.1     YES DHCP   up                    up
        FastEthernet0/1        unassigned      YES NVRAM  up                    down

R-1#sh ip dhcp binding
        Bindings from all pools not associated with VRF:
        IP address          Client-ID/              Lease expiration        Type
                            Hardware address/
                            User name
        192.168.1.1         0063.6973.636f.2d30.    Mar 01 2015 08:04 AM    Automatic
                            3031.632e.3538.3038.
                            2e66.6638.652d.4661.
                            302f.30
```

TASK :

- Enable DHCP snooping on SW1 for vlan 10
- SW1 should store the binding database in flash with the filename DHCP.txt.

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 10
SW1(config)#ip dhcp snooping database flash:DHCP.txt
SW1(config)#end
```

```
SW1#sh ip dhcp snooping
        Switch DHCP snooping is enabled
        DHCP snooping is configured on following VLANs:
        10
        Insertion of option 82 is enabled
        Option 82 on untrusted port is not allowed
        Verification of hwaddr field is enabled
        Interface                  Trusted     Rate limit (pps)
        -----------------------    -------     ----------------

SW1#debug  ip dhcp snooping agent
SW1#debug  ip dhcp snooping packet
```

TASK : Release IP address on R3 client and verify if client can get IP address from DHCP server.

```
DCHPClient#release dhcp f0/0

DCHPClient#sh ip int brief
        Interface              IP-Address      OK? Method Status              Protocol
        FastEthernet0/0        unassigned      YES DHCP   up                  up
        FastEthernet0/1        unassigned      YES NVRAM  up                  down

DCHPClient(config)#int f0/0
DCHPClient(config-if)#shutdown
DCHPClient(config-if)#no shutdown
DCHPClient(config-if)#end

00:51:19: DHCPSN: Found ingress pkt on Fa0/3 VLAN 10
00:51:19: DHCPSN: DHCP packet being sent to PI snooping process
00:51:19: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet
0/3)
00:51:19: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input
interface: Fa0/3, MAC da: ffff.ffff.ffff, MAC sa: 001c.5808.ff8e, IP da: 255.255.255.255, IP sa: 0.0.0.0,
DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP
chaddr: 001c.5808.ff8e
00:51:19: DHCP_SNOOPING: add relay information option.
00:51:19: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
00:51:19: DHCP_SNOOPING: binary dump of relay info option, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0xA 0x0 0x2 0x2 0x8 0x0 0x6 0x0 0xB 0xBE 0xE2 0xFA 0x0
00:51:19: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, pac          ket
is flooded to ingress VLAN: (10)
00:51:19: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan10.
```

00:51:20: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
00:51:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed s
tate to up
00:51:23: DHCPSN: Found ingress pkt on Fa0/3 VLAN 10
00:51:23: DHCPSN: DHCP packet being sent to PI snooping process

DCHPClient#sh ip int brief

Interface	IP-Address	OK? Method	Status	Protocol
FastEthernet0/0	unassigned	YES DHCP	up	up
FastEthernet0/1	unassigned	YES NVRAM	up	down

- Client is not able to get ip address from DHCP as by default once we enable DHCP snooping all the ports will be treated as untrusted and switch do not allow DHCP offer messanges on untrusted ports.
- We need to configure the ports connecting to DHCP as trusted so that I can forward DHCP offer messages

SW1(config)#int f0/1
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#exit

One more issue that with IOS DHCP servers is the switch inserts the option but leaves the "giaddr" field at zero.
Thus, a DHCP Server may assume that option has been formatted incorrectly, because a DHCP Relay is supposed to set the "giaddr" field to its own IP address.
An IOS DHCP server will reject by default such DHCP messages.

To overcome this issue, you may use one of the following methods:

1. Instruct the IOS DHCP Server to accept DHCP messages with a zero "giaddr" by using the global command ip dhcp relay information trust-all or the interface-level command ip dhcp relay information trusted .
2. Configure the DHCP Snooping feature in the switch not to insert Option 82. This is accomplished by using the command no ip dhcp-snooping information option.Trust the port where you receive the original DHCP message. The DHCP Snooping feature does not insert any Information Option into the received packets.

SW1(config)#no ip dhcp snooping information option

DCHPClient#
*Feb 28 08:54:49.983: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP address 192.168.1.1, mask 255.255.255.0, hostname DCHPClient

DCHPClient#sh ip int brief

Interface	IP-Address	OK? Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES DHCP	up	up

FastEthernet0/1 unassigned YES NVRAM up down

SW1#
01:00:18: %SYS-5-CONFIG_I: Configured from console by vty1 (192.168.1.10)
01:00:37: DHCP_SNOOPING: checking expired snoop binding entries
01:00:38: DHCPSN: Found ingress pkt on Fa0/3 VLAN 10
01:00:38: DHCPSN: DHCP packet being sent to PI snooping process
01:00:38: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/3)
01:00:38: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Fa0/3, MAC da: ffff.ffff.ffff, MAC sa: 001c.5808.ff8e, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 001c.5808.ff8e
01:00:38: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (10)
01:00:38: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan10.
01:00:38: DHCP_SNOOPING_SW: bridge packet send packet to port: FastEthernet0/1.
01:00:38: DHCPSN: Found ingress pkt on Fa0/1 VLAN 10
01:00:38: DHCPSN: DHCP packet being sent to PI snooping process
01:00:38: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/1)
01:00:38: DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Fa0/1, MAC da: ffff.ffff.ffff, MAC sa: 0019.aa1d.8596, IP da: 255.255.255.255, IP sa: 192.168.1.100, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.1.1, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 001c.5808.ff8e
.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 001c.5808.ff8e
01:00:42: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded

to ingress VLAN: (10)
01:00:42: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan10.
01:00:42: DHCP_SNOOPING_SW: bridge packet send packet to port: FastEthernet0/1.
01:00:42: DHCPSN: Found ingress pkt on Fa0/1 VLAN 10
01:00:42: DHCPSN: DHCP packet being sent to PI snooping process
01:00:42: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/1)
01:00:42: DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface:

Fa0/1, MAC da: ffff.ffff.ffff, MAC sa: 0019.aa1d.8596, IP da: 255.255.255.255, IP sa: 192.168.1.100, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.1.1, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr:

001c.5808.ff8e
01:00:42: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/3.
01:00:42: DHCPSN: Found ingress pkt on Fa0/3 VLAN 10
01:00:42: DHCPSN: DHCP packet being sent to PI snooping process
01:00:42: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/3)

01:00:42: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST, input interface:

Fa0/3, MAC da: ffff.ffff.ffff, MAC sa: 001c.5808.ff8e, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr:

0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 001c.5808.ff8e
01:00:42: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded

to ingress VLAN: (10)
01:00:42: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan10.
01:00:42: DHCP_SNOOPING_SW: bridge packet send packet to port: FastEthernet0/1.
01:00:42: DHCPSN: Found ingress pkt on Fa0/1 VLAN 10
01:00:42: DHCPSN: DHCP packet being sent to PI snooping process
01:00:42: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/1)
01:00:42: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Fa0/1, MAC da: ffff.ffff.ffff, MAC sa: 0019.aa1d.8596, IP da: 255.255.255.255, IP sa: 192.168.1.100, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.1.1, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 001c.5808.ff8e
01:00:42: DHCP_SNOOPING: add binding on port FastEthernet0/3.
01:00:42: DHCP_SNOOPING: added entry to table (index 82)
01:00:42: DHCP_SNOOPING: dump binding entry: Mac=00:1C:58:08:FF:8E Ip=192.168.1.1 Lease=86400 Id Type=dhcp-snooping Vlan=10 If=FastEthernet0/3
01:00:42: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/3.

SW1#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled

Interface	Trusted	Rate limit (pps)
FastEthernet0/1	yes	unlimited

SW1#sh ip dhcp snooping binding

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:1C:58:08:FF:8E	192.168.1.1	86338	dhcp-snooping	10	FastEthernet0/3

Total number of bindings: 1

SW1#sh ip dhcp snooping database

Agent URL : flash:DHCP.txt
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 112 (00:01:52)
Abort Timer Expiry : Not Running

Last Succeded Time : 00:30:24 UTC Mon Mar 1 1993
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts :	1	Startup Failures :	0
Successful Transfers :	1	Failed Transfers :	0
Successful Reads :	0	Failed Reads :	0
Successful Writes :	1	Failed Writes :	0
Media Failures :	0		

SW1#sh flash:

Directory of flash:/

```
  2  -rwx        322   Jan 1 1970 00:05:09 +00:00  system_env_vars
  3  -rwx        984   Mar 1 1993 00:01:19 +00:00  vlan.dat
  5  -rwx    6917476   Mar 1 1993 00:22:16 +00:00  c3550-ipservicesk9-mz.122-25.sec2.bin
  7  drwx        128   Mar 1 1993 00:12:36 +00:00  c3550-i9q3l2-mz.121-11.EA1
 20  -rwx       2795   Mar 1 1993 00:50:20 +00:00  config.text
 22  -rwx         13   Jan 1 1970 00:05:09 +00:00  env_vars
 23  -rwx         47   Mar 1 1993 00:30:24 +00:00  DHCP.txt
 26  -rwx         24   Mar 1 1993 00:50:21 +00:00  private-config.text
15998976 bytes total (7676416 bytes free)
```

SW1#more flash:DHCP.txt

```
2b9160f5
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.168.1.1 10 001c.5808.ff8e 2B92B1BA Fa0/3                    4d39d55b
END
```

TASK :

- Configure a Rouge DHCP server on R2 (connecting on f0/2)
- SW1 f0/2 is default in in untrusted port and it should not get IP addrss from DHCP rogue server.

R2-RougeDHCP(config)#int f0/0

```
R2-RougeDHCP(config-if)#ip address 192.168.1.200 255.255.255.0
R2-RougeDHCP(config-if)#no shutdown
R2-RougeDHCP(config-if)#end

R2-RougeDHCP(config)#ip dhcp pool ROUGE
R2-RougeDHCP(dhcp-config)#network 192.168.1.0  255.255.255.0
R2-RougeDHCP(dhcp-config)#default-router  192.168.1.200
R2-RougeDHCP(dhcp-config)#exit

DCHPClient#release dhcp f0/0

DCHPClient#sh ip int brief
        Interface              IP-Address      OK? Method Status                Protocol
        FastEthernet0/0        unassigned      YES DHCP   up                    up
        FastEthernet0/1        unassigned      YES NVRAM  up                    down

DCHPClient(config)#int f0/0
DCHPClient(config-if)#shutdown
DCHPClient(config-if)#no shutdown
DCHPClient(config-if)#end

*Feb 28 10:01:15.167: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP address
192.168.1.5, mask 255.255.255.0, hostname DCHPClient
```

TASK :

- Shutdown the interface f0/1 connecting to dhcp server.
- verify again by releasing IP address on Client .

```
SW1(config)#int f0/1
SW1(config-if)#shutdown
SW1(config-if)#exit

DCHPClient#release dhcp f0/0

DCHPClient#sh ip int brief
        Interface              IP-Address      OK? Method Status                Protocol
        FastEthernet0/0        unassigned      YES DHCP   up                    up
        FastEthernet0/1        unassigned      YES NVRAM  up                    down

DCHPClient(config)#int f0/0
DCHPClient(config-if)#shutdown
DCHPClient(config-if)#no shutdown

DCHPClient#sh ip int brief
```

```
Interface              IP-Address      OK? Method Status            Protocol
FastEthernet0/0        unassigned      YES DHCP   up                up
FastEthernet0/1        unassigned      YES NVRAM  up                down
```

TASK :

- Remove the IP DHCP snooping configuration from switch and verify the client.

```
SW1(config)#no ip dhcp snooping
SW1(config)#no ip dhcp snooping vlan 10
SW1(config)#no ip dhcp snooping database flash:DHCP.txt
SW1(config)#exit

SW1(config)#int f0/1
SW1(config-if)#no ip dhcp snooping trust
SW1(config-if)#end

DCHPClient#release dhcp f0/0

DCHPClient(config)#int f0/0
DCHPClient(config-if)#shutdown
DCHPClient(config-if)#no shutdown

DCHPClient#sh ip int brief
Interface              IP-Address      OK? Method Status            Protocol
FastEthernet0/0        192.168.1.1     YES DHCP   up                up
FastEthernet0/1        unassigned      YES NVRAM  up                down
```

- Now the client will be getting the IP address from the rouge DHCP server as the valid DHCP server is down and there is no DHCP snooping configured.
- we configured gateway on rouge dhCP server to 192.168.1.200. to test and verify disable IP routing and Trace

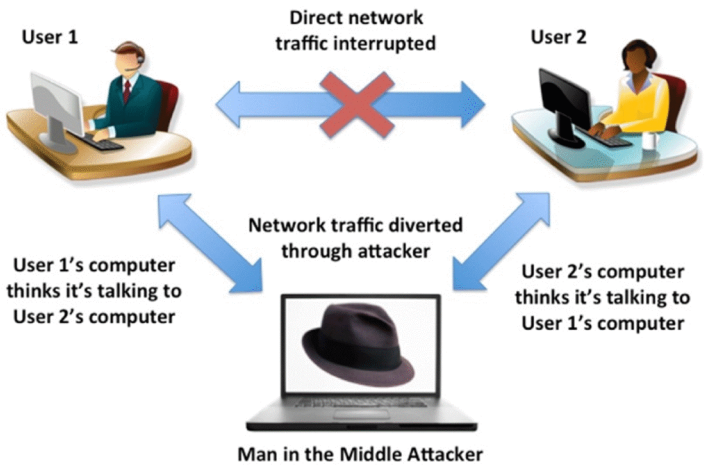
```
DCHPClient(config)#no ip routing
DCHPClient(config)#exit

DCHPClient#traceroute 172.16.1.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1
 1 192.168.1.200 0 msec 0 msec 4 msec
 2 192.168.1.200 !H  *  !H
```

TASK : Reconfigure IP dhcp snooping and prevent the client from getting IP address and gateway from rouge DHCP ensure that Client is reachable to Valid DHCP server.

```
SW1(config)#int f0/1
```

```
SW1(config-if)#no shutdown
SW1(config-if)#end

SW1(config)# ip dhcp snooping
SW1(config)#  ip dhcp snooping vlan 10
SW1(config)#  ip dhcp snooping database flash:DHCP.txt
SW1(config)#  no ip dhcp snooping information option

SW1(config)#int f0/1
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#end

DCHPClient#release dhcp f0/0

DCHPClient(config)#int f0/0
DCHPClient(config-if)#shutdown
DCHPClient(config-if)#no shutdown
DCHPClient(config-if)#end

DCHPClient#sh ip int brief
        Interface              IP-Address      OK? Method Status                Protocol
        FastEthernet0/0        192.168.1.5     YES DHCP   up                    up
        FastEthernet0/1        unassigned      YES NVRAM  up                    down

DCHPClient#traceroute 172.16.1.1
        Type escape sequence to abort.
        Tracing the route to 172.16.1.1
         1 192.168.1.100 1000 msec 0 msec 0 msec
         2 192.168.1.100 !H  *  !H

SW1#sh ip dhcp snooping
        Switch DHCP snooping is enabled
        DHCP snooping is configured on following VLANs:
        10
        Insertion of option 82 is disabled
        Option 82 on untrusted port is not allowed
        Verification of hwaddr field is enabled
        Interface                Trusted    Rate limit (pps)
        -----------------------  -------    ----------------
        FastEthernet0/1            yes          unlimited
```

IP spoofing Attack

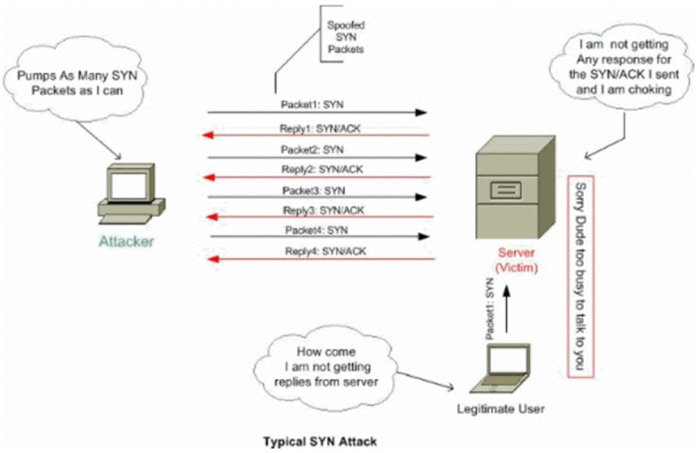


TCP Sync Flooding Attack

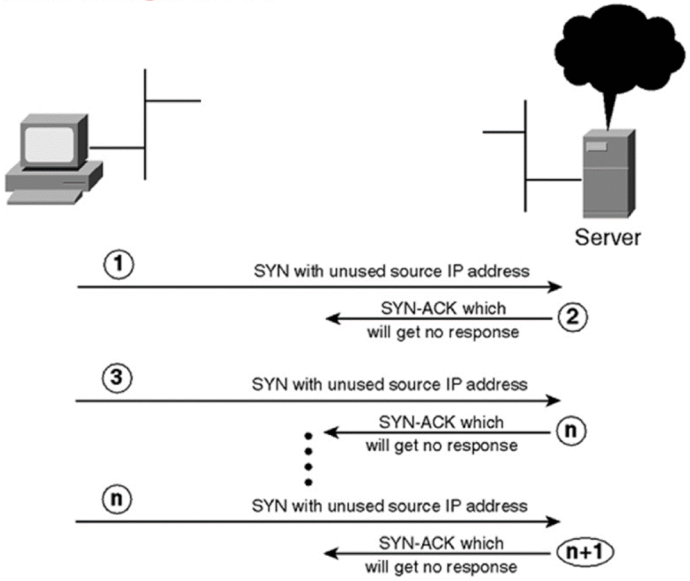
- Attacker floods with numerous TCP sync with Unused IP address.**(IP Spoofing)**
- Server busy responding by could not find source

Result :

- Denial of service
- Bandwidth utilization.



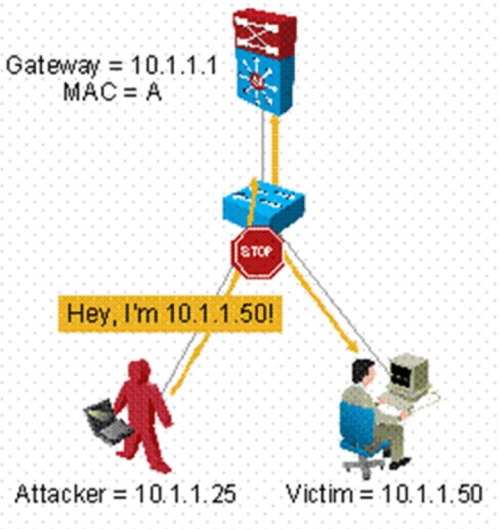
TCP Sync Flooding Attack



IP Source Guard

- prevent IP packet spoofing and TCP sync Flooding Attacks in LAN
- Validates the Correct source IP & mac address
- Accept the packets with source IP addresses matching bindings created for the port.
- For Binding uses DHCP Snooping information or can bind IP to port manually

IP source guard is configured on untrusted L2 interfaces



Configuring IP Source Guard

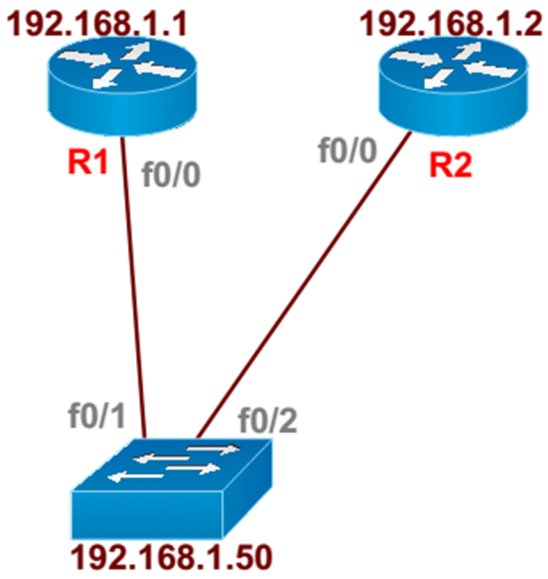
Switch(config)# **interface f0/1**
Switch(config-if)# **switchport Mode access**

Switch(config-if)# **Switchport access vlan 10**
Switch(config-if)# **switchport Port-security**
Switch(config-if)# **ip verify source port-security**

Switch(config)# **IP source binding** 0000.0000.1111 **vlan 10** 192.168.1.1 **interface** f0/1

Switch(config)# **ip dhcp snooping**
Switch(config)# **ip dhcp snooping vlan 10**

LAB : IP Source Guard ;



TASK :

- Connect topology and assign ip addressing as per the diagram.
- create vlan 10 and assign all ports connecting in vlan 10

```
SW1(config)# vlan 10

SW1(config)# int range f0/1 - 2
SW1(config-if-range)#  switchport mode access
SW1(config-if-range)#  switchport access vlan 10
SW1(config-if-range)# spanning-tree portfast
SW1(config-if-range)#exit

SW1(config)#int vlan 10
SW1(config-if)# ip address 192.168.1.50 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#end

R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#exit

R2(config)#int f0/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#exit

R1#ping 192.168.1.2
        Type escape sequence to abort.
```

Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping 192.168.1.50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

TASK ;

- Configure SW1 to prevent IP address spoofing on f0/1 - 2 interfaces.
- Enforce Layer 2 filtering for the MAC addresses corresponding to secured IP addresses at the same time.

```
SW1(config)#  int range f0/1 - 2
SW1(config-if-range)#  switchport port-security
SW1(config-if-range)#  ip verify source port-security
SW1(config-if-range)#exit

SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 10
SW1(config)#end
```

- Once you enable IP Source Guard, the switch only permits IP packets that match the DHCP snooping database or static IP to MAC addresses and port bindings.
- The switch also allows ingress DHCP packets for hosts to obtain IP addresses.
- IP Source Guard relieves you from the need of applying any IP ingress filtering on individual ports to prevent IP address spoofing.
- The switch filters packets based onboththe source IP and MAC addresses, and the secure MAC address is taken from the DHCP snooping database or a static mapping entry.
- You may enable IP Source Guard on a trunk port as well.
- In this case, DHCP snooping must be enabled on all trunked VLANs for filtering to work properly.

SW1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/200/1000 ms

SW1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/201/1000 ms

SW1#sh ip arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.50	-	000b.bee2.fa00	ARPA	Vlan10
Internet	192.168.1.10	0	a4ba.dbbe.d185	ARPA	Vlan10
Internet	192.168.1.1	0	0019.aa1d.8596	ARPA	Vlan10
Internet	192.168.1.2	0	0018.73c3.0b20	ARPA	Vlan10

SW1(config)#ip source binding 0019.aa1d.8596 vlan 10 192.168.1.1 interface f0/1
SW1(config)#ip source binding 0018.73c3.0b20 vlan 10 192.168.1.2 interface f0/2
SW1(config)#end

SW1#sh ip source binding

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:19:AA:1D:85:96	192.168.1.1	infinite	static	10	FastEthernet0/1
00:18:73:C3:0B:20	192.168.1.2	infinite	static	10	FastEthernet0/1

Total number of bindings: 2

R1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#SW1#sh ip verify source

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
Fa0/1	ip-mac	active	192.168.1.1	00:19:AA:1D:85:96	10
Fa0/2	ip-mac	active	192.168.1.2	00:18:73:C3:0B:20	10

Ensure that filtering actually prevents IP address spoofing by changing the IP on R1

R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.5 255.255.255.0
R1(config-if)#exit

R1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

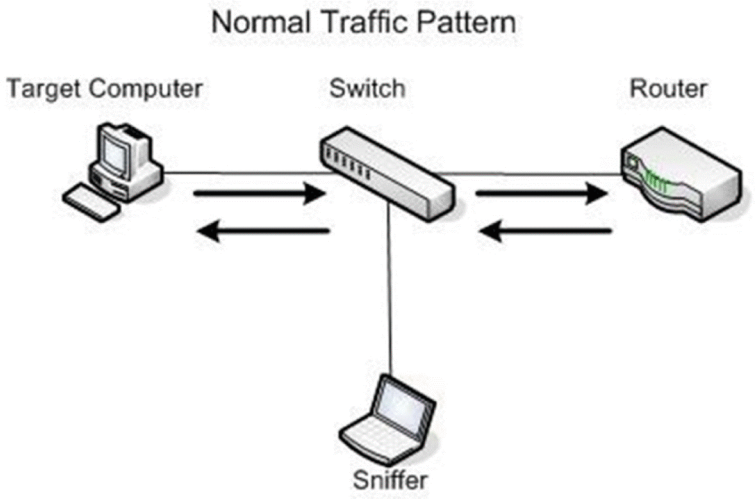
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#exit

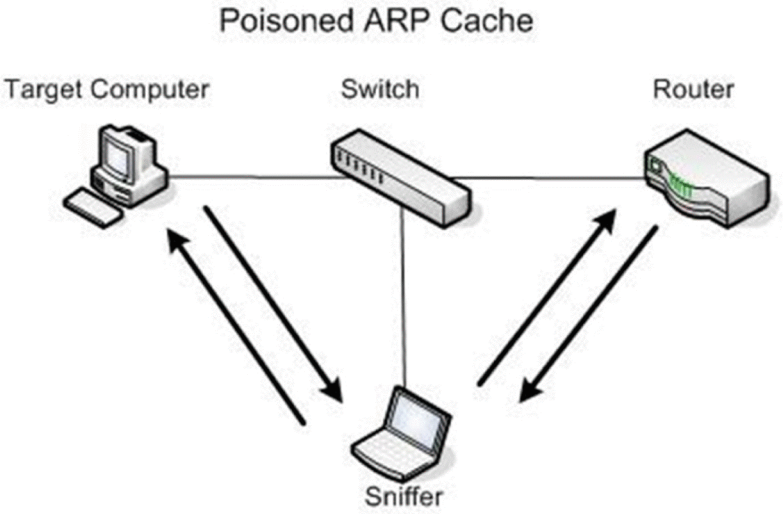
R1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

ARP Spoofing



ARP Spoofing

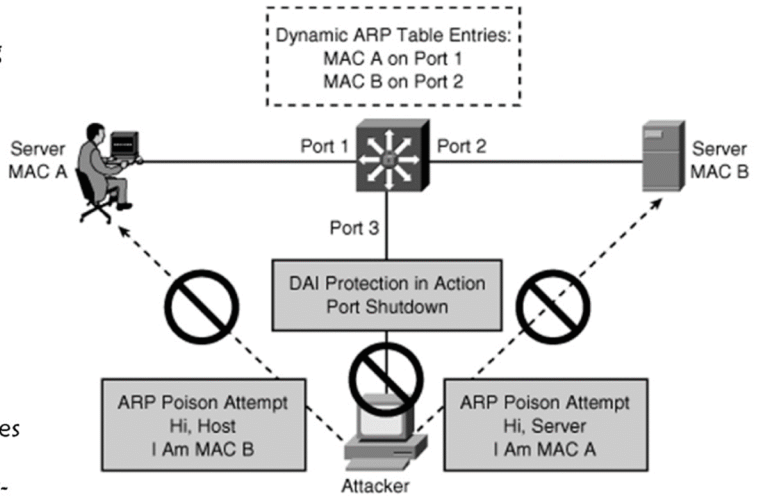


Dynamic ARP Inspection

- Prevents from ARP spoofing attacks
- Creates a special IP to MAC address binding table in the switch.
- This table is dynamically built based on the DHCP snooping database contents

or

- You can also add static entries to the database manually using ARP Inspection access-lists.



- DAI associates each interface with a trusted state or an untrusted state.
- Trusted interfaces bypass all DAI.
- Untrusted interfaces undergo DAI validation.

DAI (Mac to IP binding)

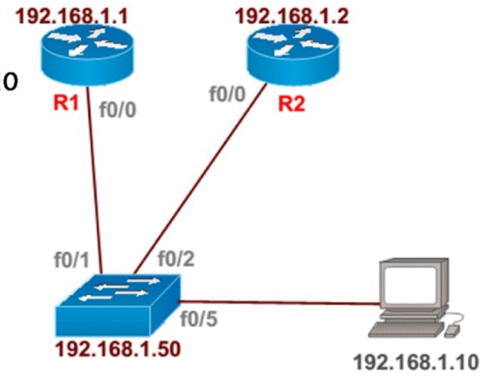
- When enabled by default, the IP ARP Inspection feature builds all ARP mapping information based on the DHCP bindings table.
- If there are hosts on the segment not using DHCP for address allocation, you must configure ARP accesslists.

```
SW1(config)#arp access-list ARP_VLAN10
SW1(config-arp-nacl)#  permit ip host 192.168.1.1 mac host 0019.aa1d.8596 log
SW1(config-arp-nacl)#  permit ip host 192.168.1.2 mac host  0018.73c3.0b20 log
SW1(config-arp-nacl)#exit
```

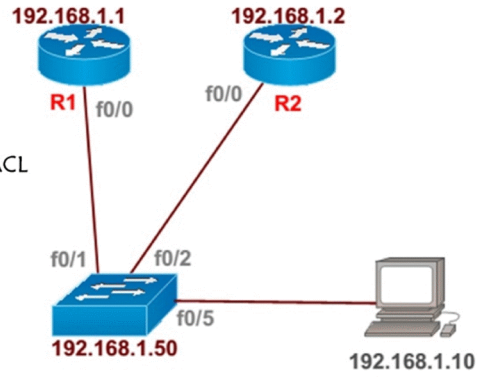
```
SW1(config)#ip arp inspection vlan 10
SW1(config)#ip arp inspection filter  ARP_VLAN10 vlan 10
```

Dynamic ARP Inspection Configuration

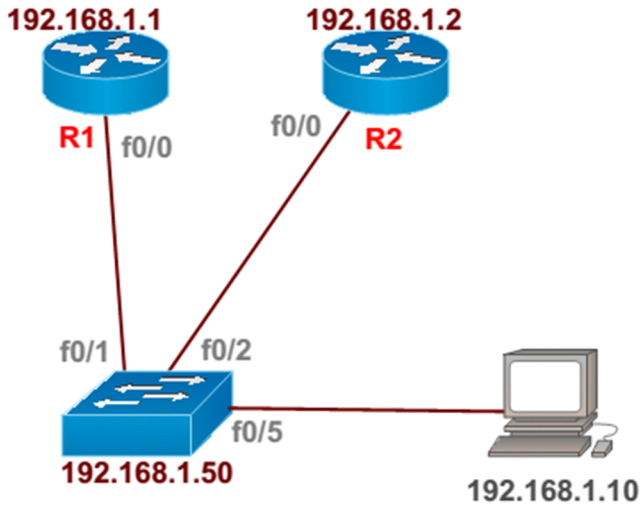
```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 10
SW1(config)#exit

SW1(config)#arp access-list ARP_VLAN10
SW1(config-arp-nacl)#  permit ip host 192.168.1.1 mac host 0019.aa1d.8596 log
SW1(config-arp-nacl)#  permit ip host 192.168.1.2 mac host  0018.73c3.0b20 log
SW1(config-arp-nacl)#exit

SW1(config)#ip arp inspection vlan 10
SW1(config)#ip arp inspection filter  ARP_VLAN10 vlan 10

SW1(config)#int f0/5
SW1(config-if)#ip arp inspection trust
SW1(config-if)#end
```




```
SW1#sh ip arp inspection vlan 10
 Source Mac Validation      : Disabled
 Destination Mac Validation : Disabled
 IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match     Static ACL
 ----     -------------    ---------   ---------     ----------
   10     Enabled          Active      ARP_VLAN10    No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
   10     Deny             Deny
```



LAB : Dynamic ARP inspection:



TASK :

- Configure f0/1 - 2 connecting to R1/R2 as access ports in vlan 10
- Connect topology and assign ip addressing as per the diagram.
- create vlan 10 and assign all ports connecting in vlan 10

```
SW1(config)# vlan 10

SW1(config)#int vlan 10
SW1(config-if)# ip address 192.168.1.50 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#end

SW1(config)# int range f0/1 - 2
SW1(config-if-range)#  switchport mode access
SW1(config-if-range)#  switchport access vlan 10
SW1(config-if-range)# spanning-tree portfast
SW1(config-if-range)#exit

R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#exit

R2(config)#int f0/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#exit

R1#ping 192.168.1.2
        Type escape sequence to abort.
```

Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping 192.168.1.50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

TASK :

- Configure SW1 to prevent ARP poisoning attacks on VLAN 10,
- Without configuring trust ports on SW1, ensure it enforces ARP security for SW2 and SW3.

SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 10
SW1(config)#exit

SW1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

SW1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

SW1#sh ip arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.50	-	000b.bee2.fa00	ARPA	Vlan10
Internet	192.168.1.10	0	a4ba.dbbe.d185	ARPA	Vlan10
Internet	192.168.1.1	36	0019.aa1d.8596	ARPA	Vlan10
Internet	192.168.1.2	71	0018.73c3.0b20	ARPA	Vlan10

SW1(config)#arp access-list ARP_VLAN10
SW1(config-arp-nacl)# permit ip host 192.168.1.1 mac host 0019.aa1d.8596 log
SW1(config-arp-nacl)# permit ip host 192.168.1.2 mac host 0018.73c3.0b20 log
SW1(config-arp-nacl)#permit ip host 192.168.1.10 mac host a4ba.dbbe.d185 log
SW1(config-arp-nacl)#exit

NOTE :

- Here f0/5 port is connecting to my PC and i am accessing routers via telnet.
- To ensure that this port should not go with DAI inspection we can configure this port as trusted port.
- Or we can add entry of my PC mac (a4ba.dbbe.d185) binded to ip address 192.168.1.10 in ARP access-list

- Note that implementing ARP Inspection may break some services, such as Proxy ARP.
- To resolve these issues, ARP Inspection allows you to configure some ports as trusted for ARP Inspection.
- On trusted ports, the switch does not inspect any ARP message. It is common to trust ARP messages on switch uplink ports, pointing toward the network core.

```
SW1(config)#int f0/5
SW1(config-if)#ip arp inspection trust
SW1(config-if)#end
```

- When the switch receives an ARP packet on an ARP-untrusted (the default state) port, it inspects the packet contents.
- Based on the IP to MAC address binding information in the packet, the switch permits the packet only if it matches the ARP Inspection table. This prevents ARP poisoning attacks.

```
SW1(config)#ip arp inspection vlan 10
SW1(config)#ip arp inspection filter  ARP_VLAN10 vlan 10

SW1#sh ip arp inspection vlan 10
        Source Mac Validation      : Disabled
        Destination Mac Validation : Disabled
        IP Address Validation      : Disabled

         Vlan     Configuration    Operation   ACL Match         Static ACL
         ----     -------------    ---------   ---------         ----------
           10     Enabled          Active      ARP_VLAN10        No

         Vlan     ACL Logging      DHCP Logging
         ----     -----------      ------------
           10     Deny             Deny

SW1#clear arp-cache

R1#ping 192.168.1.1
        Type escape sequence to abort.
        Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

R1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#ping 192.168.1.50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.50, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

R1#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

- Change the MAC address entry for R1 on VLAN 10 interface and observe how the switch denies the violating ARP packets.
- As you can see, there is no DHCP snooping entry to match the new SW2 MAC address, so the ARP packets are dropped by the switch.

SW1#sh arp access-list

ARP access list ARP_VLAN10
permit ip host 192.168.1.1 mac host 0019.aa1d.8596 log
permit ip host 192.168.1.2 mac host 0018.73c3.0b20 log
permit ip host 192.168.1.10 mac host a4ba.dbbe.d185 log

SW1(config)#arp access-list ARP_VLAN10
SW1(config-arp-nacl)#no permit ip host 192.168.1.1 mac host 0019.aa1d.8596 log
SW1(config-arp-nacl)# permit ip host 192.168.1.1 mac host aaaa.aaaa.aaaa log
SW1(config-arp-nacl)#end

R1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW1#
02:23:46: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/1, vlan 10.([0019.aa1d.8596/192.168.1.1/000b.bee2.fa00/192.168.1.50/02:23:46 UTC Mon Mar 1 1993])

02:23:46: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/1, vlan

TASK :

- Reconfigure ARP access-list back to previous stage.
- configure F0/5 port as trusted port and should not go with DAI inspection.

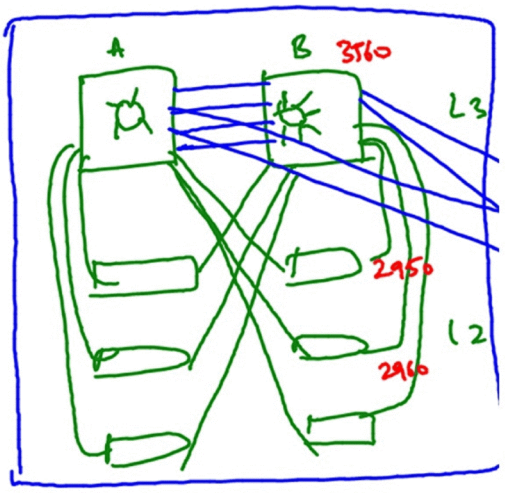
```
SW1(config)#arp access-list  ARP_VLAN10
SW1(config-arp-nacl)#no  permit ip host 192.168.1.1 mac host aaaa.aaaa.aaaa log
SW1(config-arp-nacl)#  permit ip host 192.168.1.1 mac host 0019.aa1d.8596 log
SW1(config-arp-nacl)#exit
```

Storm Control

broadcast storms occurs when packets flood the LAN, creating excessive traffic and degrading network performance.

- STP failure or misconfiguration
- unicast storms created by faulty host NICs.

- Broadcast, multicast, or unicast packets are flooded on all ports in the same VLAN.
- These storms can increase the CPU utilization on a switch to 100%, reducing the performance of the network.



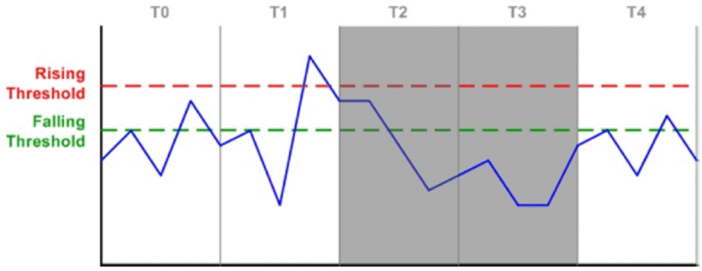
Storm Control

Storm control is used to limit the amount of unicast, multicast, or broadcast traffic received inbound on a port.

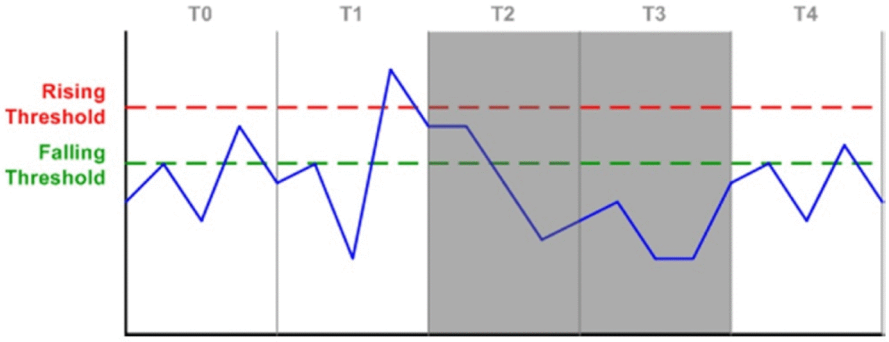
- Monitor multicast/broadcast/unicast traffic & Suppress it.
- Done on port basis.

Actions :

1. slow it down
2. put port to error disable State.



Storm Control



Suppression thresholds in three types:

1. bandwidth as a percentage of the physical interface
2. traffic rate in packets per second
3. traffic rate in bits per second

Storm Control Configuration

Switch(config-if)# **storm-control broadcast level** 75 60
Switch(config-if)# **storm-control multicast level pps** 1000 500
Switch(config-if)# **storm-control action shutdown**

SW1#sh storm-control broadcast

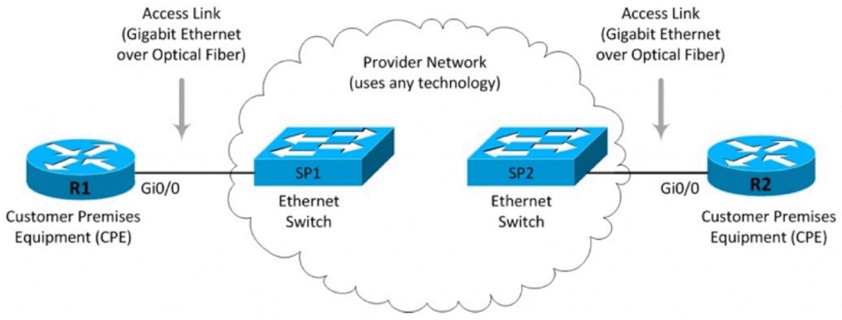
Interface	Filter State	Upper	Lower	Current
Fa0/2	Link Down	75.00%	60.00%	0.00%

SW1#sh storm-control multicast

Interface	Filter State	Upper	Lower	Current
Fa0/2	Link Down	1k pps	500 pps	0 pps

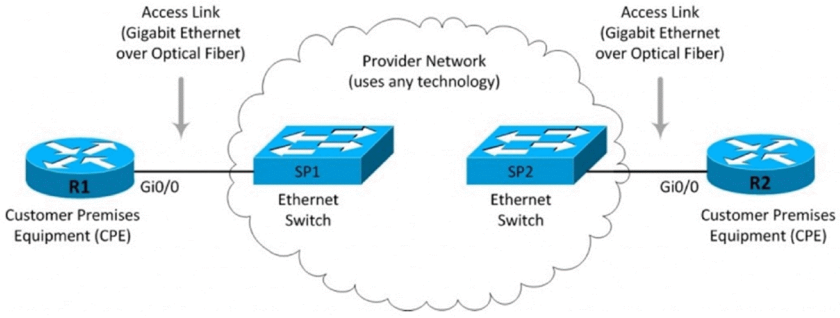
Metro Ethernet lines

- Initially Ethernet was only restricted to LAN (distance limits)
- Use fiber Standards support for longer distances.
- Overcome both speed and Distance limits.
- Service providers started using Ethernet in WAN.



Advantages

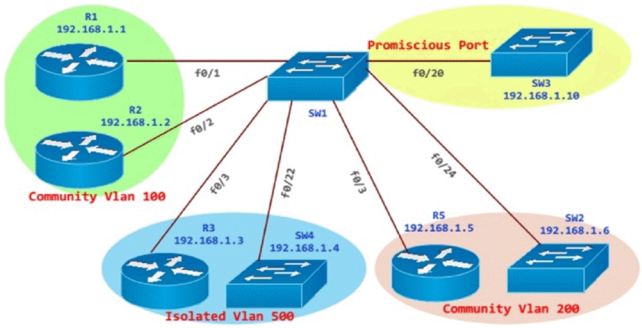
- Support high Speeds up to 100 Mpbs or 1 Gbps (Frame relay upto 44 Mbps)
- Customer end uses Ethernet Interface (Instead of Serial)



Private VLAN

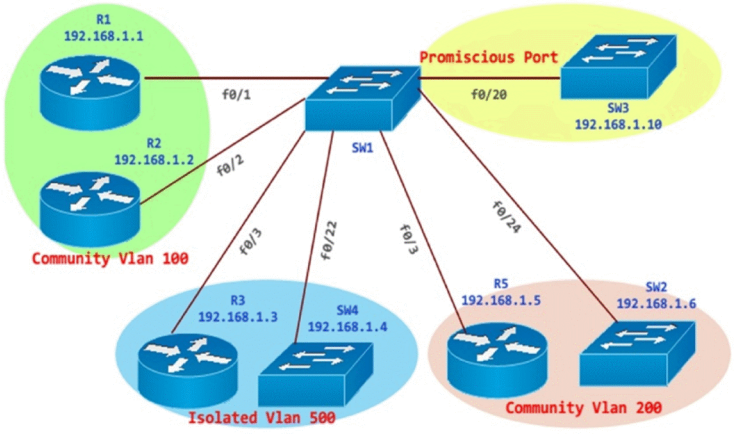
Addresses two problems that service providers face when using VLANs.

1. switch supports up to 1005 active VLANs. If a service provider assigns one VLAN per customer, this limits the numbers of customers the service provider can support.
2. To enable IP routing, each VLAN is assigned a subnet address space or a block of addresses, which can result in wasting the unused IP addresses, and cause IP address management problems.



Private VLAN

- Using private VLANs provides scalability and IP address management benefits for service providers and Layer 2 security for customers.
- Private VLANs partition a regular VLAN domain into subdomains.
- A subdomain is represented by a pair of VLANs: a primary VLAN and a secondary VLAN.



There are two types of secondary VLANs:

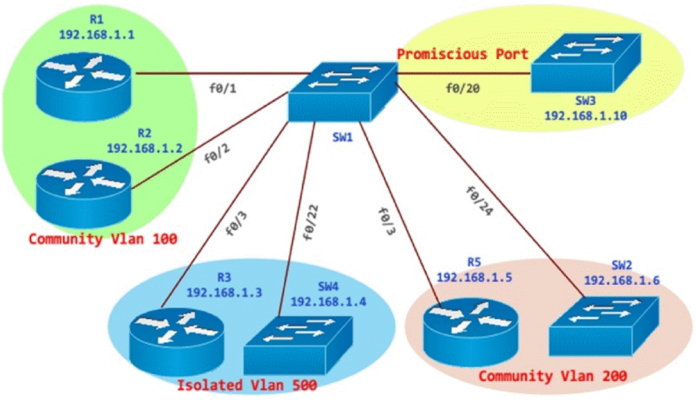
Isolated VLANs :

- Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.

Community VLANs :

- Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level.

Promiscuous
Port attaches to a router, firewall, etc; can communicate with all hosts (including isolated and community ports)



Private VLAN

Advantage :

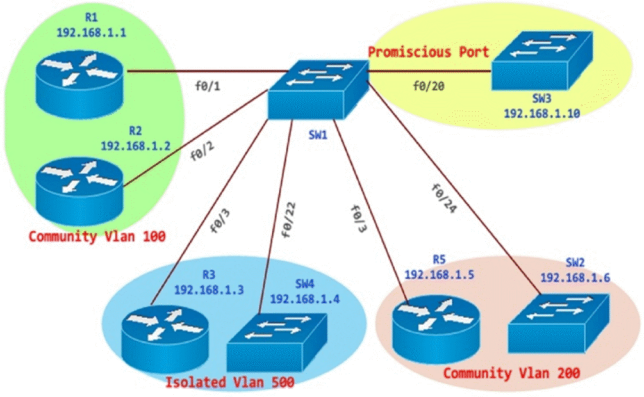
- Reduce VLAN and IP subnet consumption;
- you can prevent traffic between end stations even though they are in the same VLAN and IP subnet

Metro Ethernet Switches

ME 3400 ,catalyst 3750 ,
ME3800X, ME 4900,

Private VLAN Configuration

```
SW1(config)#vtp mode transparent

SW1(config)#vlan 10
SW1(config-vlan)#private-vlan primary
SW1(config-vlan)#exit

SW1(config)#vlan 100
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit
SW1(config)#vlan 200
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit
SW1(config)#vlan 500
SW1(config-vlan)#private-vlan isolated
SW1(config-vlan)#end
```

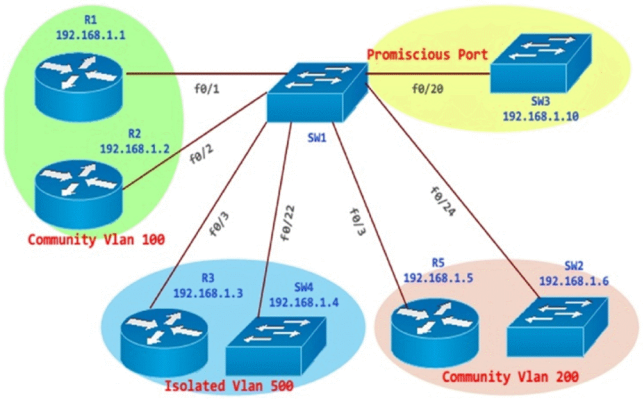


Note: Isolated VLAN can be only one and Community VLAN can be many

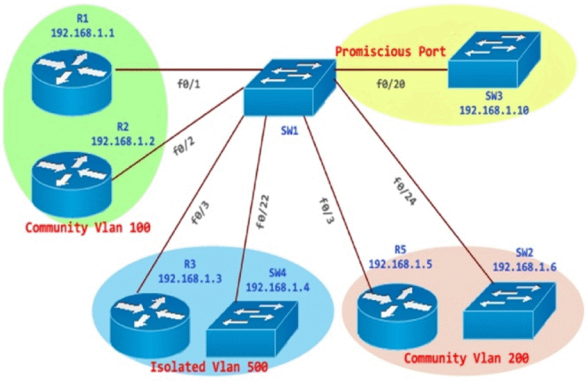
SW1(config)#vlan 10
SW1(config-vlan)#private-vlan association ?
  WORD VLAN IDs of the private VLANs to be configured
  add Add a VLAN to private VLAN list
  remove Remove a VLAN from private VLAN list
SW1(config-vlan)#private-vlan association add 100,200,500
SW1(config-vlan)#end

SW1#sh vlan private-vlan

Primary	Secondary	Type	Ports
10	100	community	
10	200	community	
10	500	isolated	

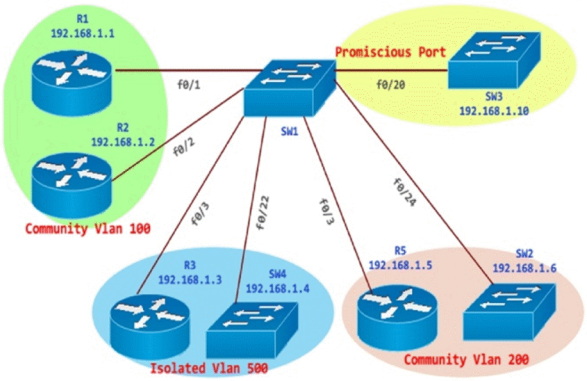


Configuring Promiscuous Port



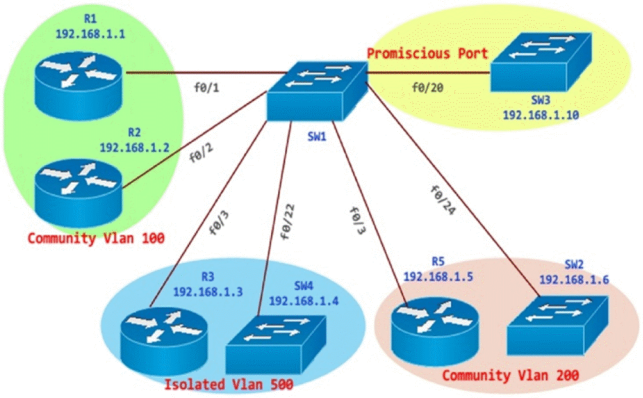
SW1(config)#int f0/20
SW1(config-if)#switchport mode private-vlan promiscuous
SW1(config-if)#switchport private-vlan mapping 10 100,200,500
SW1(config-if)#end

Configuring Community Secondary VLAN



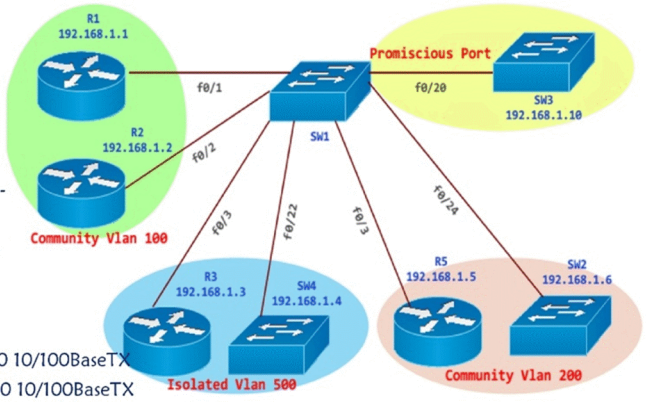

```
SW1(config)#int range f0/1 - 2
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 100

SW1(config)#int range f0/5 , f0/24
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 200
```

Configuring Isolated Secondary VLAN




```
SW1(config)#int range f0/3 , f0/22
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 500
SW1(config-if-range)#end
```

Private VLAN Verification



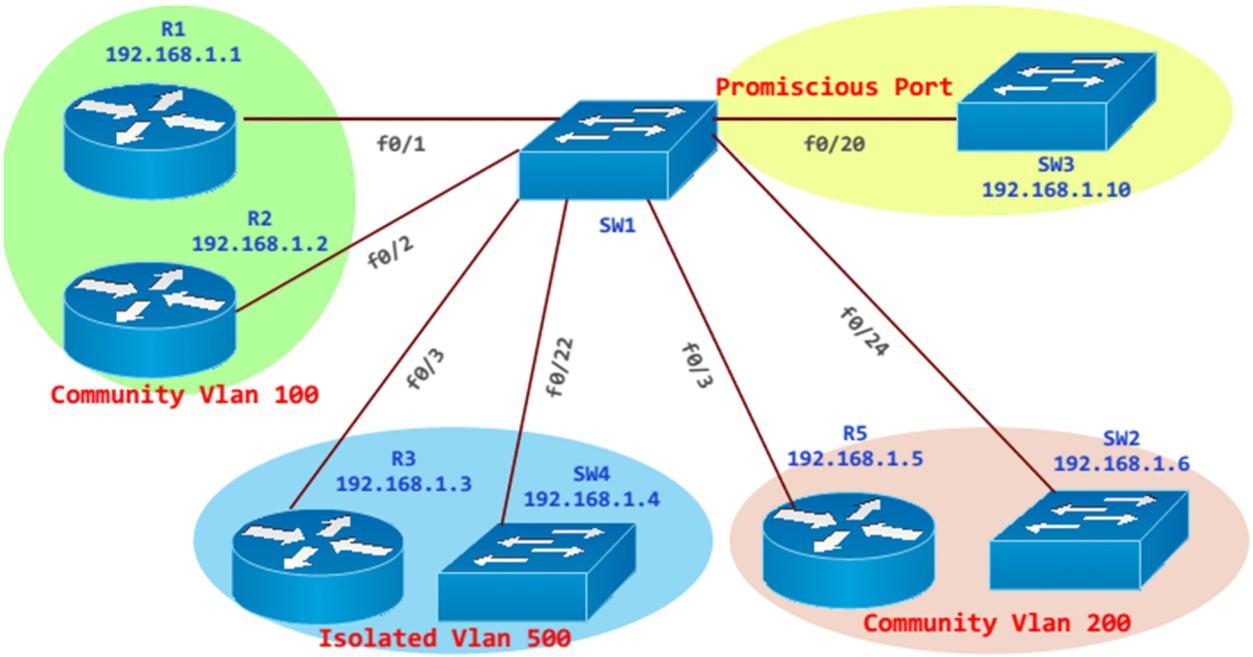
SW1#sh vlan private-vlan

Primary	Secondary	Type	Ports
10	100	community	Fa0/1, Fa0/2, Fa0/20
10	200	community	Fa0/5, Fa0/20, Fa0/24
10	500	isolated	Fa0/3, Fa0/20, Fa0/22

SW1#sh interfaces status | in connected

Fa0/1	connected	10,100	a-full	a-100 10/100BaseTX
Fa0/2	connected	10,100	a-full	a-100 10/100BaseTX
Fa0/3	connected	10,500	a-full	a-100 10/100BaseTX
Fa0/5	connected	10,200	a-full	a-100 10/100BaseTX
Fa0/20	connected	10	a-full	a-100 10/100BaseTX
Fa0/22	connected	10,500	a-full	a-100 10/100BaseTX
Fa0/24	connected	10,200	a-full	a-100 10/100BaseTX

LAB: PRIVATE VLAN



TASK:

- Configure VTP mode as transparent and all ports connecting to end devices in vlan 10 (primary vlan)
- Create vlan 100, 200 , 500 and configure vlan 100 and 200 as community vlan-type and vlan 500 as isolated vlan-type
- VLAN 100. 200.500 will be acting as secondary vlans and associate them to primary vlan 10

```
SW1(config)#interface range f0/1 -3 , f0/5, f0/20 , f0/22, f0/24
SW1(config-if-range)#no shutdown
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
```

```
SW1#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/21, Fa0/22
                                                 Fa0/23, Gi0/1, Gi0/2
10   VLAN0010                          active    Fa0/1, Fa0/2, Fa0/3,
                                                 Fa0/5, Fa0/20, Fa0/22, Fa0/24
```

```
SW3(config)#int f0/20
SW3(config-if)#no switchport
SW3(config-if)#ip add 192.168.1.10 255.255.255.0
SW3(config-if)#no shut
SW3(config-if)#end

SW2(config)#int f0/24
SW2(config-if)#no switchport
SW2(config-if)#ip add 192.168.1.6 255.255.255.0
SW2(config-if)#no sh
SW2(config-if)#end

R-1(config)#int g0/0
R-1(config-if)#ip add 192.168.1.1 255.255.255.0
R-1(config-if)#no sh
R-1(config-if)#end

R-2(config)#int g0/0
R-2(config-if)#ip add 192.168.1.2 255.255.255.0
R-2(config-if)#no sh
R-2(config-if)#end

R-3(config)#int g0/0
R-3(config-if)#ip add 192.168.1.3 255.255.255.0
R-3(config-if)#no sh
R-3(config-if)#end

SW4(config)#int f0/22
SW4(config-if)#no switchport
SW4(config-if)#ip add 192.168.1.4 255.255.255.0
SW4(config-if)#no sh
SW4(config-if)#end

R-5(config)#int g0/0
R-5(config-if)#ip add 192.168.1.5  255.255.255.0
R-5(config-if)#no sh
R-5(config-if)#end

R-5#ping 192.168.1.1
        Type escape sequence to abort.
        Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
        .!!!!
        Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

R-5#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

R-5#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

R-5#ping 192.168.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/2/4 ms

R-5#ping 192.168.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R-5#ping 192.168.1.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R-5#ping 192.168.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/1 ms

R-5#ping 192.168.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R-5#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:

..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/1 ms

SW1

```
SW1(config)#vtp mode transparent

SW1(config)#vlan 10
SW1(config-vlan)#private-vlan primary
SW1(config-vlan)#exit

SW1(config)#vlan 100
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit

SW1(config)#vlan 200
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit

SW1(config)#vlan 500
SW1(config-vlan)#private-vlan isolated
SW1(config-vlan)#end
```

Note:

- Isolated VLAN can be only one and Community VLAN can be many
- Here VLAN 10 is the primary VLAN and VLAN 100. 200.500 will be acting as secondary vlans associated to primary vlan (VLAN 10) with the following command :

```
SW1(config)#vlan 10
SW1(config-vlan)#private-vlan association ?
        WORD    VLAN IDs of the private VLANs to be configured
        add     Add a VLAN to private VLAN list
        remove  Remove a VLAN from private VLAN list

SW1(config-vlan)#private-vlan association add 100,200,500
SW1(config-vlan)#end

SW1#sh vlan private-vlan
        Primary Secondary Type            Ports
        ------- --------- ----------------- ------------------------------------------
        10      100       community
        10      200       community
        10      500       isolated
```

TASK: Configure the port fa0/20 as Promiscuous as it needs to be accessed by all vlan.

```
SW1(config)#int f0/20
SW1(config-if)#switchport mode private-vlan ?
        host         Set the mode to private-vlan host
        promiscuous  Set the mode to private-vlan promiscuous

SW1(config-if)#switchport mode private-vlan promiscuous

SW1(config-if)#switchport private-vlan association ?
        host     Set the private VLAN host association
        mapping  Set the private VLAN promiscuous mapping

SW1(config-if)#switchport private-vlan mapping 10 100,200,500
SW1(config-if)#end
```

The above command assign the port to primary Vlan and maps the vlan 100, 200 , 500 .

TASK:

- Configure the port fa0/1 and fa0/2 to separate community so that they can talk to each other and promiscuous port

```
SW1(config)#int range f0/1 - 2
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 100
SW1(config-if-range)#end
```

The above command assigns fa0/1 and fa0/2 to a separate community 100 as these two can communicate with each other and fa0/20 (promiscuous port)

TASK:

- Configure the port fa0/24 and fa0/5 to separate community so that they can talk to each other and promiscuous port

```
SW1(config)#int range f0/5 , f0/24
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 200
SW1(config-if-range)#end
```

The above command assigns fa0/5 and fa0/24 to a separate community 200 as these two can communicate with each other and fa0/20 (promiscuous port).

TASK

- Configure the port fa0/3 and fa0/22 so that they cannot talk to each other but they can talk to fa0/20 (promiscuous port)

```
SW1(config)#int range f0/3 , f0/22
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 500
SW1(config-if-range)#end
```

The above command assigns fa0/3 and fa0/22 as ISOLATED ports configured as Vlan 500 and these two cannot communicate with each other but can talk to gateway port fa0/20 (promiscuous port).

```
SW1#sh vlan private-vlan
        Primary Secondary Type            Ports
        ------- --------- ----------------- ------------------------------------------
        10      100       community         Fa0/1, Fa0/2, Fa0/20
        10      200       community         Fa0/5, Fa0/20, Fa0/24
        10      500       isolated          Fa0/3, Fa0/20, Fa0/22

SW1#sh interfaces status | in connected
        Fa0/1                connected    10,100     a-full  a-100 10/100BaseTX
        Fa0/2                connected    10,100     a-full  a-100 10/100BaseTX
        Fa0/3                connected    10,500     a-full  a-100 10/100BaseTX
        Fa0/5                connected    10,200     a-full  a-100 10/100BaseTX
        Fa0/20               connected    10         a-full  a-100 10/100BaseTX
        Fa0/22               connected    10,500     a-full  a-100 10/100BaseTX
        Fa0/24               connected    10,200     a-full  a-100 10/100BaseTX

SW3#ping 192.168.1.1
        Type escape sequence to abort.
        Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 1/200/1000 ms

SW3#ping 192.168.1.2
        Type escape sequence to abort.
        Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 1/201/1000 ms

SW3#ping 192.168.1.3
        Type escape sequence to abort.
        Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 1/201/1000 ms
```

SW3#ping 192.168.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

SW3#ping 192.168.1.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

SW3#ping 192.168.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

R-1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

R-1#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R-1#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-1#ping 192.168.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-1#ping 192.168.1.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-1#ping 192.168.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R-2#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R-2#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-2#ping 192.168.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-2#ping 192.168.1.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-2#ping 192.168.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)

R-3#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R-3#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-3#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-3#ping 192.168.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-3#ping 192.168.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-3#ping 192.168.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW4#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

SW4#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW4#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW4#ping 192.168.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW4#ping 192.168.1.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW4#ping 192.168.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-5#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R-5#ping 192.168.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R-5#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-5#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-5#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R-5#ping 192.168.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW2#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

SW2#ping 192.168.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

SW2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW2#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)

SW2#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW2#ping 192.168.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

First Hop Redundancy Protocols

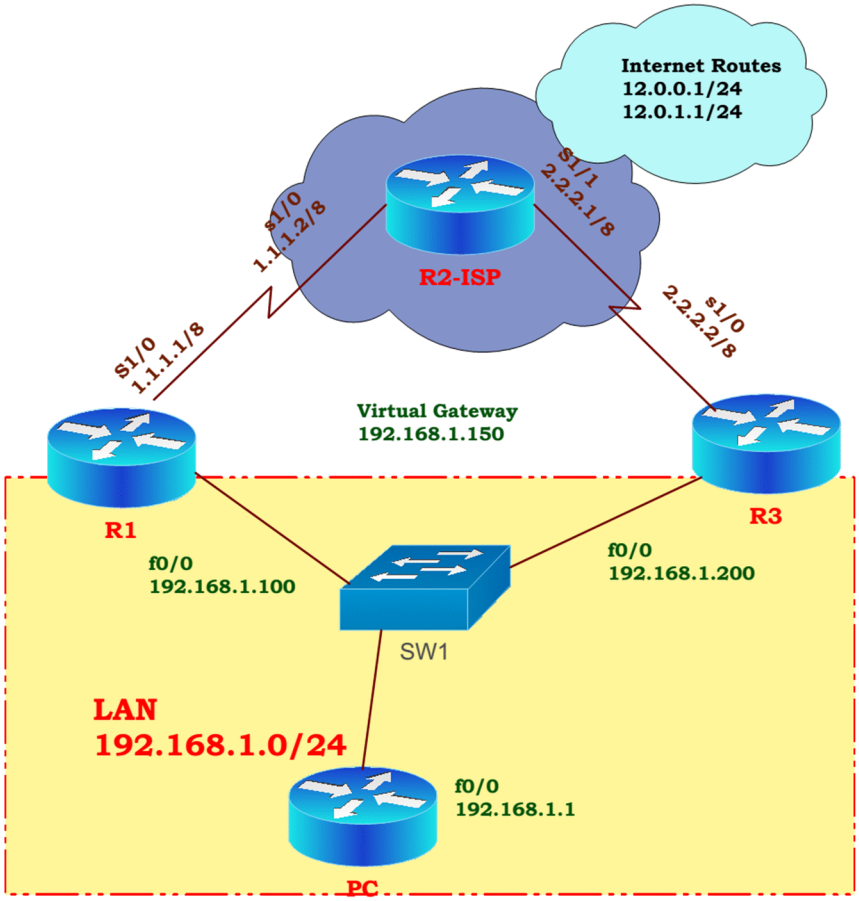
HSRP , VRRP , GLBP

	HSRP	VRRP	GLBP
Scope	Cisco Proprietary	IEEE standard	Cisco proprietary
Standard	RFC2281	RFC3768	none
Load Balancing	No	No	Yes
Multicast Group IP address	224.0.0.2 in ver 1 224.0.0.102 in ver 2	224.0.0.18	224.0.0.102
Transport PortNumber	UDP 1985	UDP 112	UDP 3222
Timers	Hello – 3 sec	Advertisement – 1 sec	Hello – 3sec
	Hold – 10 sec	Master down time = 3*Advertisement Time + Skew TimeSkew Time = (256- Priority)/256	Hold – 10sec

	HSRP	VRRP	GLBP
Election	Active Router:1.Highest Priority2. Highest IP address (Tiebreaker)	Master Router: (*) 1-Highest Priority 2-Highest IP (Tiebreaker)	Active Virtual Gateway: 1-Highest Priority 2-Highest IP (Tiebreaker)
Router Role	One Active Router one Standby Router- one or more listening Routers	One Active Router One or More Backup Routers	-One AVG (Active Virtual Gateway) up to 4 AVF Routers on the group (Active VirtualForwarder) passing traffic.- up to 1024 virtual Routers (GLBP groups) per physical interface.

	HSRP	VRRP	GLBP
Preempt	By default Preempt is disabled If Active Router(Highest Priority) is down and up again, Preempt should be configured to become a Active Router again	By default Preempt is ON in VRRP. If Active Router is down and up again, It will automatically become a Master Router	By default Preempt is disabled If Active Router(Highest Priority) is down and up again, Preempt should be configured to become a Active Router again.
Group Virtual Mac Address	0000.0c07.acxx	0000.5e00.01xx	0007.b4xx.xxxx
IPv6 support	Version 2	Version 3	Yes

LAB: HOT STANDBY ROUTER PROTOCOL (HSRP)



TASK:

- Configure the Basic IP addressing on Routers as per the Diagram & test Connectivity
- Configure Default Route on R1/R3 to reach routes on Internet
- Configure Static Route on R2-ISP back to LAN network on both Sides

```
R1(config)#int f0/0
R1(config-if)#ip add 192.168.1.100 255.255.255.0
R1(config-if)#no sh
R1(config-if)#end

R3(config)#int f0/0
R3(config-if)#ip add 192.168.1.200 255.255.255.0
R3(config-if)#no sh

R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2

R3(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

R2(config)#ip route 192.168.1.0 255.255.255.0  1.1.1.1
```

R2(config)#ip route 192.168.1.0 255.255.255.0 2.2.2.2

R3#ping 192.168.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/45/96 ms

TASK:

- Configure HSRP on R1 and R3 under f0/0 and use Virtual Gateway IP address as 192.168.1.150/24.
- Make sure that R1 becomes primary and R2 as backup.
- Active Gateway Priority 120 and the Standby are left at the default.
- Authentication between both switches - md5 – password "cisco
- Standby will take up active role in a 5 seconds incase if 5 hello packets not received
- The primary gateway should have the ability to resume the Primary role once primary router or track interface is reachable (preempt)
- Make sure that the reachability to internet should be established even if the WAN interface (R1 s1/0) goes down

```
R1(config)#int fa0/0
R1(config-if)#standby 12 ip 192.168.1.150
R1(config-if)#standby 12 priority 120
R1(config-if)#standby 12 preempt
R1(config-if)#standby 12 authentication md5 key-string cisco
R1(config-if)#standby 12 track s1/0   30
R1(config-if)#standby 12 timers 1   5

R3(config)#int fa0/0
R3(config-if)#standby 12 ip 192.168.1.150
R3(config-if)#standby 12 preempt
R3(config-if)# standby 12 authentication md5 key-string cisco
R3(config-if)#standby  12 timers 1 5
```

R1#sh standby

```
FastEthernet0/0 - Group 12
  State is Active
    2 state changes, last state change 00:03:03
  Virtual IP address is 192.168.1.150
  Active virtual MAC address is 0000.0c07.ac0c
    Local virtual MAC address is 0000.0c07.ac0c (v1 default)
  Hello time 1 sec, hold time 5 sec
    Next hello sent in 0.720 secs
  Authentication MD5, key-string "cisco"
  Preemption enabled
  Active router is local
```

```
  Standby router is 192.168.1.200, priority 100 (expires in 4.724 sec)
  Priority 120 (configured 120)
    Track interface Serial1/0 state Up decrement 30
  IP redundancy name is "hsrp-Fa0/0-12" (default)
```

R1#sh standby brief

```
                P indicates configured to preempt.
                |Interface   Grp Prio P State    Active          Standby         Virtual IP
Fa0/0           12  120  P Active   local           192.168.1.200   192.168.1.150
```

R3#sh standby

```
FastEthernet0/0 - Group 12
  State is Standby
    4 state changes, last state change 00:05:55
  Virtual IP address is 192.168.1.150
  Active virtual MAC address is 0000.0c07.ac0c
    Local virtual MAC address is 0000.0c07.ac0c (v1 default)
  Hello time 1 sec, hold time 5 sec
    Next hello sent in 0.252 secs
  Authentication MD5, key-string "cisco"
  Preemption enabled
- Active router is 192.168.1.100, priority 120 (expires in 4.524 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Fa0/0-12" (default)
```

R3#sh standby brief

```
                P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Fa0/0       12  100  P Standby  192.168.1.100   local           192.168.1.150
```

TASK:

- Assuming the router R4 as the PC connected in LAN,Configure Client routers for Verification in the LAN

On R4

```
Client1(config)#hostname Client-R4
Client-R4(config)#no ip routing

Client-R4(config)#int f0/0
Client-R4(config-if)#ip add 192.168.1.1 255.255.255.0
Client-R4(config-if)#exit

Client-R4(config)#ip default-gateway 192.168.1.150
```

Client-R4(config)#end

Client-R4#ping 192.168.1.150

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/237/1108 ms

Client-R4#ping 192.168.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/215/1036 ms

Client-R4#ping 192.168.1.200

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/225/1052 ms

Client-R4#traceroute 12.0.0.1

Type escape sequence to abort.
Tracing the route to 12.0.0.1
1 192.168.1.100 48 msec 120 msec 28 msec
2 1.1.1.2 40 msec 144 msec *

R1(config)#int f0/0
R1(config-if)#shutdown

Client1#ping 12.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/72/172 ms

Client1#traceroute 12.0.0.1

Type escape sequence to abort.
Tracing the route to 12.0.0.1

1 192.168.1.200 168 msec 108 msec 44 msec
2 2.2.2.1 108 msec 172 msec

R3#sh standby

```
FastEthernet0/0 - Group 12
  State is Active
    2 state changes, last state change 00:00:06
  Virtual IP address is 192.168.1.150
  Active virtual MAC address is 0000.0c07.ac0c
    Local virtual MAC address is 0000.0c07.ac0c (v1 default)
  Hello time 1 sec, hold time 5 sec
    Next hello sent in 0.244 secs
  Authentication MD5, key-string "cisco"
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Fa0/0-12" (default)
```

```
R1(config)#int f0/0
R1(config-if)#no shutdown
R1(config-if)#end
```

```
R3#sh standby
        FastEthernet0/0 - Group 12
          State is Standby
            4 state changes, last state change 00:00:07
          Virtual IP address is 192.168.1.150
          Active virtual MAC address is 0000.0c07.ac0c
            Local virtual MAC address is 0000.0c07.ac0c (v1 default)
          Hello time 1 sec, hold time 5 sec
            Next hello sent in 0.316 secs
          Authentication MD5, key-string "cisco"
          Preemption enabled
          Active router is 192.168.1.100, priority 120 (expires in 4.380 sec)
          Standby router is local
          Priority 100 (default 100)
          IP redundancy name is "hsrp-Fa0/0-12" (default)
```

```
R1#sh standby
        FastEthernet0/0 - Group 12
          State is Active
            4 state changes, last state change 00:01:07
          Virtual IP address is 192.168.1.150
          Active virtual MAC address is 0000.0c07.ac0c
            Local virtual MAC address is 0000.0c07.ac0c (v1 default)
          Hello time 1 sec, hold time 5 sec
            Next hello sent in 0.896 secs
```

```
        Authentication MD5, key-string "cisco"
        Preemption enabled
        Active router is local
        Standby router is 192.168.1.200, priority 100 (expires in 4.912 sec)
        Priority 120 (configured 120)
          Track interface Serial1/0 state Up decrement 30
        IP redundancy name is "hsrp-Fa0/0-12" (default)

R1(config)#int s1/0
R1(config-if)#shutdown
R1(config-if)#end

R1#sh standby
      FastEthernet0/0 - Group 12
        State is Standby
          6 state changes, last state change 00:00:30
        Virtual IP address is 192.168.1.150
        Active virtual MAC address is 0000.0c07.ac0c
          Local virtual MAC address is 0000.0c07.ac0c (v1 default)
        Hello time 1 sec, hold time 5 sec
          Next hello sent in 0.648 secs
        Authentication MD5, key-string "cisco"
        Preemption enabled
        Active router is 192.168.1.200, priority 100 (expires in 4.740 sec)
        Standby router is local
        Priority 90 (configured 120)
          Track interface Serial1/0 state Down decrement 30
        IP redundancy name is "hsrp-Fa0/0-12" (default)
R1(config)#int s1/0
R1(config-if)#no shutdown
R1(config-if)#end

R1#sh standby
      FastEthernet0/0 - Group 12
        State is Active
          7 state changes, last state change 00:00:11
        Virtual IP address is 192.168.1.150
        Active virtual MAC address is 0000.0c07.ac0c
          Local virtual MAC address is 0000.0c07.ac0c (v1 default)
        Hello time 1 sec, hold time 5 sec
          Next hello sent in 0.876 secs
        Authentication MD5, key-string "cisco"
        Preemption enabled
        Active router is local
```

Standby router is 192.168.1.200; priority 100 (expires in 4.964 sec)
Priority 120 (configured 120)
Track interface Serial1/0 state Up decrement 30
IP redundancy name is "hsrp-Fa0/0-12" (default)

TASK

- Configure R1 to track the default route and make sure that you should be able to reach internet (R2 loopbacks) even if the default route goes down on R1

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 1.1.1.2 to network 0.0.0.0

C    1.0.0.0/8 is directly connected, Serial1/0
     11.0.0.0/24 is subnetted, 4 subnets
C       11.0.3.0 is directly connected, Loopback3
C       11.0.2.0 is directly connected, Loopback2
C       11.0.1.0 is directly connected, Loopback1
C       11.0.0.0 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 1.1.1.2
```

```
R1(config)#int f0/0
R1(config-if)#no standby 12 track Serial1/0 30
R1(config-if)#exit

R1(config)#track 1 ip route  0.0.0.0  0.0.0.0 reachability

R1(config)#int f0/0
R1(config-if)#standby 12 track 1 decrement 30

R1#sh run | in track
 track 1 ip route 0.0.0.0 0.0.0.0 reachability
  standby 12 track 1 decrement 30

R1#sh standby
 FastEthernet0/0 - Group 12
   State is Active
```

```
  7 state changes, last state change 00:08:13
 Virtual IP address is 192.168.1.150
 Active virtual MAC address is 0000.0c07.ac0c
   Local virtual MAC address is 0000.0c07.ac0c (v1 default)
 Hello time 1 sec, hold time 5 sec
   Next hello sent in 0.164 secs
 Authentication MD5, key-string "cisco"
 Preemption enabled
 Active router is local
 Standby router is 192.168.1.200; priority 100 (expires in 4.356 sec)
 Priority 120 (configured 120)
   Track object 1 state Up decrement 30
 IP redundancy name is "hsrp-Fa0/0-12" (default)
```

```
R2(config)#int s1/0
R2(config-if)#shutdown
```

```
R1#sh ip route
        Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
               D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
               N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
               E1 - OSPF external type 1, E2 - OSPF external type 2
               i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
               ia - IS-IS inter area, * - candidate default, U - per-user static route
               o - ODR, P - periodic downloaded static route

        Gateway of last resort is not set

            11.0.0.0/24 is subnetted, 4 subnets
        C       11.0.3.0 is directly connected, Loopback3
        C       11.0.2.0 is directly connected, Loopback2
        C       11.0.1.0 is directly connected, Loopback1
        C       11.0.0.0 is directly connected, Loopback0
        C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
R1#sh standby
        FastEthernet0/0 - Group 12
          State is Standby
            9 state changes, last state change 00:00:44
          Virtual IP address is 192.168.1.150
          Active virtual MAC address is 0000.0c07.ac0c
            Local virtual MAC address is 0000.0c07.ac0c (v1 default)
          Hello time 1 sec, hold time 5 sec
            Next hello sent in 0.000 secs
```

Authentication MD5, key-string "cisco"
Preemption enabled
Active router is 192.168.1.200; priority 100 (expires in 4.100 sec)
Standby router is local
Priority 90 (configured 120)
Track object 1 state Down decrement 30
IP redundancy name is "hsrp-Fa0/0-12" (default)

client-R4#traceroute 12.0.0.1
Type escape sequence to abort.
Tracing the route to 12.0.0.1

1 192.168.1.200 60 msec 88 msec 16 msec
2 2.2.2.1 88 msec 92 msec *

TASK:

- Remove the HSRP configurations done the previous task.
- Remove shutdown command from interface

R2(config)#int s1/0
R2(config-if)#shutdown

On R1 and R3

R3(config)#int f0/0
R3(config-if)#no standby 12

TASK:

- Configure HSRP on R1 and R3 F0/0 interface using Group 1 & 3.
- R1 should be Active for Group 1 and Backup for Group 3.
- R3 should be Active for Group 3 and Backup for Group 1.
- Active Gateway Priority 120 and the Standby are left at the default.
- The primary gateway should have the ability to resume the Primary role once primary router or track interface is is reachable (preempt)
- Make sure that the reachability to internet should be established even if the WAN interface of both groups (R1 & R3 s1/0) goes down

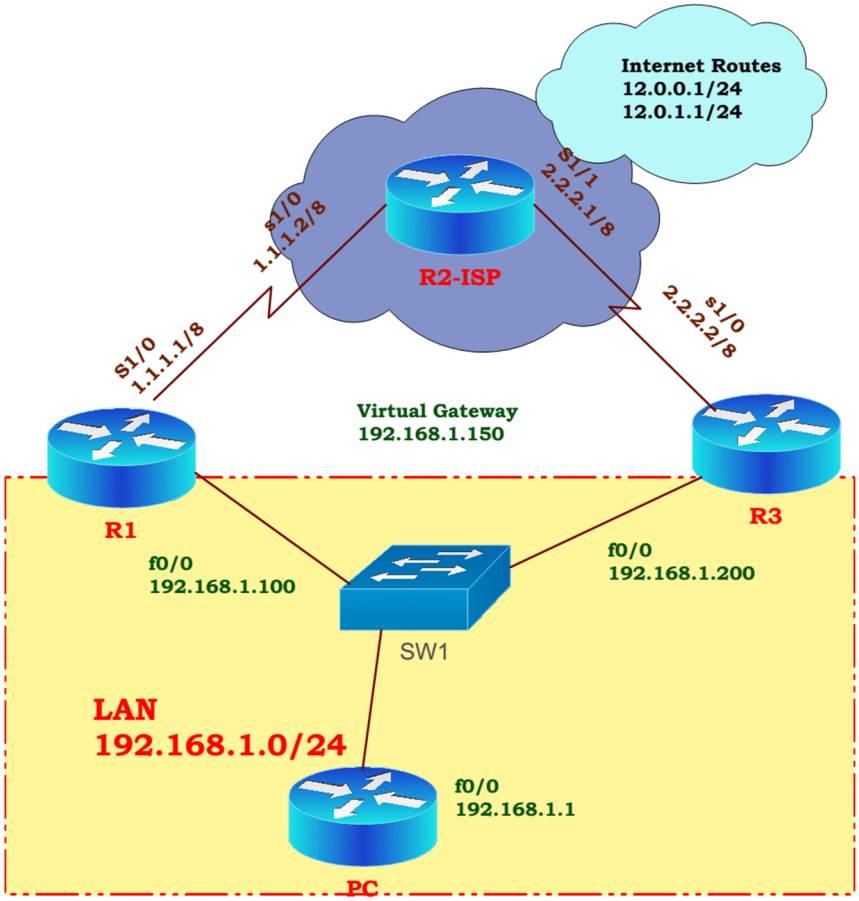
R1(config)#int fa0/0
R1(config-if)# standby 1 ip 192.168.1.150
R1(config-if)#standby 1 priority 120
R1(config-if)#standby 1 preempt
R1(config-if)# standby 1 track s1/0 30

R1(config-if)#standby 3 ip 192.168.1.160
R1(config-if)#standby 3 preempt
R1(config-if)#end

```
R3(config)#int fa0/0
R3(config-if)# standby 1 ip 192.168.1.150
R3(config-if)# standby 1 preempt

R3(config-if)#standby 3 ip 192.168.1.160
R3(config-if)#standby 3 preempt
R3(config-if)# standby 3 track s1/0 30
R3(config-if)# standby 3 priority 120
R3(config-if)#end

R1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Fa0/0       1   120  P Active   local           192.168.1.200   192.168.1.150
Fa0/0       3   100  P Standby  192.168.1.200   local           192.168.1.160

R3#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Fa0/0       1   100  P Standby  192.168.1.100   local           192.168.1.150
Fa0/0       3   120  P Active   local           192.168.1.100   192.168.1.160


R3#sh standby
FastEthernet0/0 - Group 1
  State is Standby
    1 state change, last state change 00:02:17
  Virtual IP address is 192.168.1.150
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.000 secs
  Preemption enabled
  Active router is 192.168.1.100, priority 120 (expires in 7.684 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Fa0/0-1" (default)

FastEthernet0/0 - Group 3
  State is Active
    2 state changes, last state change 00:02:02
  Virtual IP address is 192.168.1.160
```

```
  Active virtual MAC address is 0000.0c07.ac03
    Local virtual MAC address is 0000.0c07.ac03 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.836 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.100, priority 100 (expires in 7.884 sec)
  Priority 120 (configured 120)
    Track interface Serial1/0 state Up decrement 30
  IP redundancy name is "hsrp-Fa0/0-3" (default)

R1#sh standby
        FastEthernet0/0 - Group 1
          State is Active
            2 state changes, last state change 00:03:17
          Virtual IP address is 192.168.1.150
          Active virtual MAC address is 0000.0c07.ac01
            Local virtual MAC address is 0000.0c07.ac01 (v1 default)
          Hello time 3 sec, hold time 10 sec
            Next hello sent in 0.180 secs
          Preemption enabled
          Active router is local
          Standby router is 192.168.1.200, priority 100 (expires in 7.484 sec)
          Priority 120 (configured 120)
            Track interface Serial1/0 state Up decrement 30
          IP redundancy name is "hsrp-Fa0/0-1" (default)

        FastEthernet0/0 - Group 3
          State is Standby
            4 state changes, last state change 00:02:16
          Virtual IP address is 192.168.1.160
          Active virtual MAC address is 0000.0c07.ac03
            Local virtual MAC address is 0000.0c07.ac03 (v1 default)
          Hello time 3 sec, hold time 10 sec
            Next hello sent in 1.376 secs
          Preemption enabled
          Active router is 192.168.1.200; priority 120 (expires in 9.756 sec)
          Standby router is local
          Priority 100 (default 100)
          IP redundancy name is "hsrp-Fa0/0-3" (default)
```

LAB: VRRP



TASK:

- Configure HSRP on R1 and R3 under f0/0 and use Virtual Gateway IP addresses as 192.168.1.150/24.
- Make sure that R1 becomes primary and R2 as backup.
- Active Gateway Priority 120 and the Standby are left at the default.
- Authentication between both switches - md5 – password "cisco
- The primary gateway should have the ability to resume the Primary role once primary router or track interface is reachable (default preempt enabled in VRRP)
- Make sure that the reachability to internet should be established even if the WAN interface (R1 s1/0) goes down

```
R1(config)#int f0/0
R1(config-if)#vrrp 1 ip 192.168.1.150
R1(config-if)# vrrp 1 priority 120
R1(config-if)# vrrp 1 authentication md5 key-string cisco

R1(config-if)# vrrp 1 track ?
      <1-500>  Tracked object
R1(config-if)#exit
```

```
R1(config)#track  1 interface s1/0 line-protocol
R1(config)#int f0/0
R1(config-if)#vrrp 1 track 1 decrement 30
R1(config-if)#exit

R3(config)#int f0/0
R3(config-if)#vrrp 1 ip 192.168.1.150
R3(config-if)# vrrp 1 authentication md5 key-string cisco
R3(config-if)#  exit

R3#sh vrrp
    FastEthernet0/0 - Group 1
      State is Backup
      Virtual IP address is 192.168.1.150
      Virtual MAC address is 0000.5e00.0101
      Advertisement interval is 1.000 sec
      Preemption enabled
      Priority is 100
      Authentication MD5, key-string "cisco"
      Master Router is 192.168.1.100, priority is 120
      Master Advertisement interval is 1.000 sec
      Master Down interval is 3.609 sec (expires in 3.573 sec)

R3#sh vrrp brief
    Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
    Fa0/0              1   100 3609      Y  Backup  192.168.1.100   192.168.1.150

R1#sh vrrp
    FastEthernet0/0 - Group 1
      State is Master
      Virtual IP address is 192.168.1.150
      Virtual MAC address is 0000.5e00.0101
      Advertisement interval is 1.000 sec
      Preemption enabled
      Priority is 120
        Track object 1 state Up decrement 30
      Authentication MD5, key-string "cisco"
      Master Router is 192.168.1.100 (local), priority is 120
      Master Advertisement interval is 1.000 sec
      Master Down interval is 3.531 sec

R1#sh vrrp brief
    Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
```

```
Fa0/0          1   120 3531      Y  Master  192.168.1.100   192.168.1.150

R1(config)#int f0/0
R1(config-if)#shutdown
R1(config-if)#exit

R3#sh vrrp brief
     Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
     Fa0/0              1   100 3609      Y  Master  192.168.1.200   192.168.1.150



R1#sh vrrp brief
     Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
     Fa0/0              1   120 3531      Y  Master  192.168.1.100   192.168.1.150

R3#sh vrrp brief
     Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
     Fa0/0              1   100 3609      Y  Backup  192.168.1.100   192.168.1.150

R1(config)#int s1/0
R1(config-if)#shutdown
R1(config-if)#end

R1#sh vrrp brief
     Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
     Fa0/0              1   90  3531      Y  Backup  192.168.1.200   192.168.1.150

R1#sh vrrp
     FastEthernet0/0 - Group 1
       State is Backup
       Virtual IP address is 192.168.1.150
       Virtual MAC address is 0000.5e00.0101
       Advertisement interval is 1.000 sec
       Preemption enabled
       Priority is 90  (cfgd 120)
         Track object 1 state Down decrement 30
       Authentication MD5, key-string "cisco"
       Master Router is 192.168.1.200, priority is 100
       Master Advertisement interval is 1.000 sec
       Master Down interval is 3.531 sec (expires in 2.843 sec)

R3#sh vrrp brief
     Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
```

```
Fa0/0          1   100 3609      Y  Master  192.168.1.200   192.168.1.150
```

```
R3#sh vrrp
    FastEthernet0/0 - Group 1
      State is Master
      Virtual IP address is 192.168.1.150
      Virtual MAC address is 0000.5e00.0101
      Advertisement interval is 1.000 sec
      Preemption enabled
      Priority is 100
      Authentication MD5, key-string "cisco"
      Master Router is 192.168.1.200 (local), priority is 100
      Master Advertisement interval is 1.000 sec
      Master Down interval is 3.609 sec
```

```
R1(config)#int s1/0
R1(config-if)#no shutdown
R1(config-if)#end
```

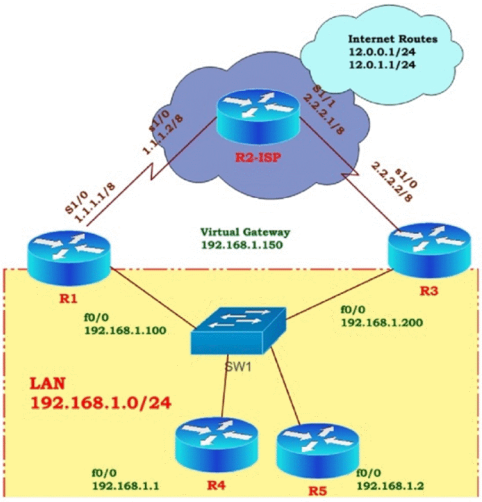
```
R1#sh vrrp brief
    Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
    Fa0/0              1   120 3531      Y  Master  192.168.1.100   192.168.1.150
```

```
R3#sh vrrp brief
    Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
    Fa0/0              1   100 3609      Y  Backup  192.168.1.100   192.168.1.150
```

Gateway Load BalancingProtocol (GLBP)

- simultaneous use of up to four gateways
- one virtual IP address. Each router has a virtual MAC address
- different routers virtual MAC addresses are sent in answer to ARPs for the virtual IP address.
- AVG assign the virtual mac address to other routers (AVF)
- AVG will answer the ARP requests for virtual IP address

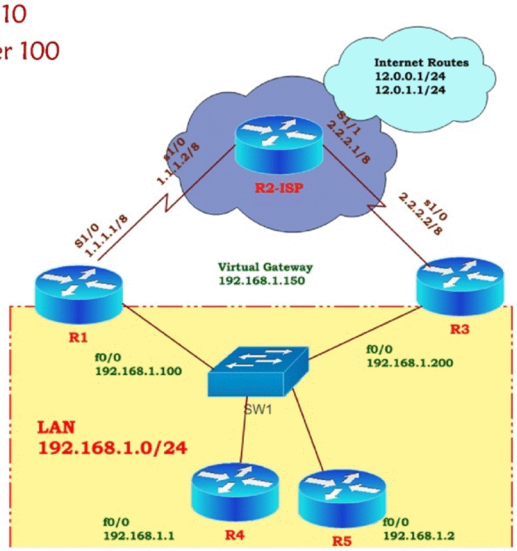
```
R1(config)# int f0/0
R1(config-if)#glbp 1 ip 192.168.1.150
R1(config-if)#glbp 1 priority 120
R1(config-if)#glbp 1 preempt
R1(config-if)#exit

R3(config)#int f0/0
R3(config-if)# glbp 1 ip 192.168.1.150
R3(config-if)# glbp 1 preempt
```



GLBP track interface :

R1(config#Track 1 int s1/0 line-protocol

R1(config)# Int f0/0
R1(config-if)# Glbp 1 weighting track 1 decrement 10
R1(config-if)# Glbp 1 weighting 100 lower 95 upper 100



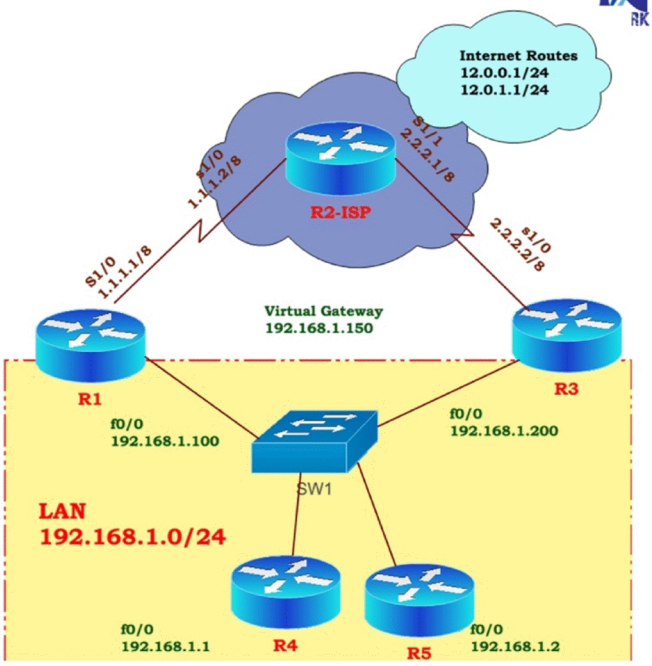
GLBP load sharing is done in one of three ways:

- Weighted load balancing:
  - Traffic is balanced proportional to a configured weight.
- Host-dependent load balancing:
  - A given host always uses the same router.
- Round-robin load balancing:
  - Each router MAC is used to respond to ARP requests in turn.

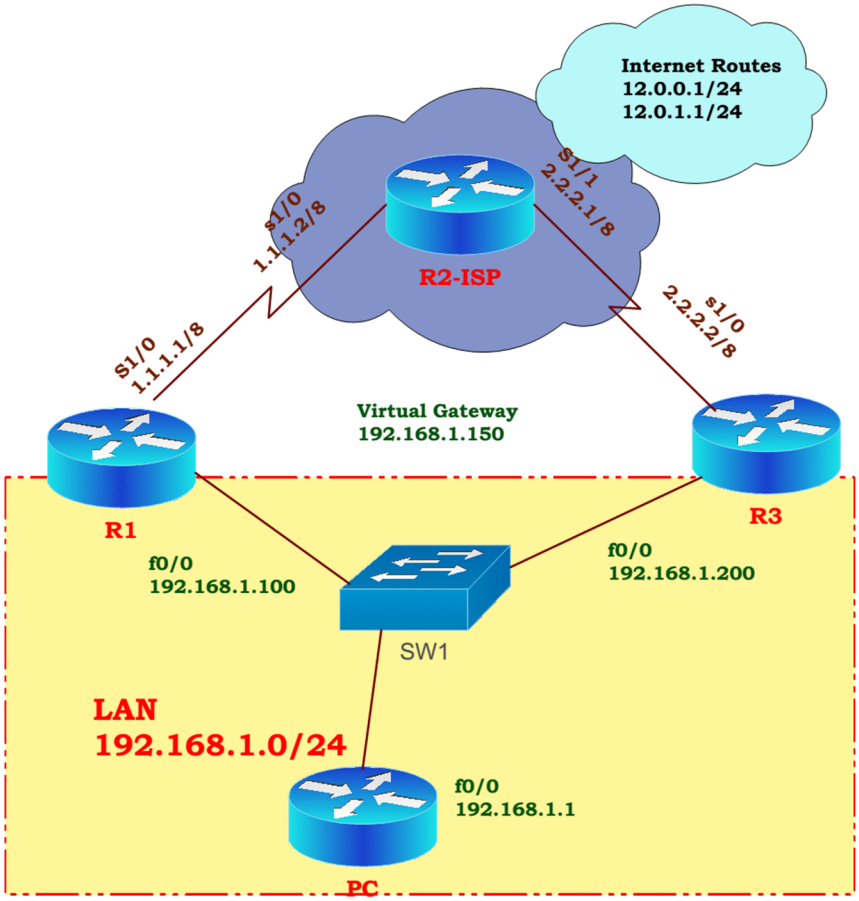
R1(config)#**int f0/0**
R1(config-if)#**glbp 1 load-balancing ?**

host-dependent Load balance equally, source MAC determines forwarder choice
round-robin Load balance equally using each forwarder in turn
weighted Load balance in proportion to forwarder weighting

GLBP



LAB: GATEWAY LOAD BALANCING PROTOCOL (GLBP)



TASK:

- Configure the Basic IP addressing on Routers as per the Diagram & test Connectivity
- Configure Default Route on R1/R3 to reach routes on Internet
- Configure Static Route on R2-ISP back to LAN network on both Sides

```
R1(config)#int f0/0
R1(config-if)#ip add 192.168.1.100 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#end

R3(config)#int f0/0
R3(config-if)#ip add 192.168.1.200 255.255.255.0
R3(config-if)#no shutdown

R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2

R3(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

R2(config)#ip route 192.168.1.0 255.255.255.0  1.1.1.1
R2(config)#ip route 192.168.1.0 255.255.255.0  2.2.2.2
```

```
R3#ping 192.168.1.100
        Type escapes sequence to abort.
        Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 28/45/96 ms
```

TASK:

- Configure GLBP on R1 and R3 under f0/0
- Make sure that R1 becomes AVG and R2 as AVF.
- Active Virtual Gateway Priority 120 and the other gateway is left at the default.
- Authentication between both switches - md5 – password "cisco"
- The AVG should have the ability to resume the Primary role once primary router or track interface is is reachable (preempt)

```
R1(config)# int f0/0
R1(config-if)#  glbp 1 authentication md5 key-string cisco
R1(config-if)#  glbp 1 preempt
R1(config-if)#  glbp 1 timers 1 3
R1(config-if)#  glbp 1 priority 120
R1(config-if)#  glbp 1 ip 192.168.1.150
R1(config-if)# exit

R3(config)#int f0/0
R3(config-if)#    glbp 1 authentication md5 key-string cisco
R3(config-if)#    glbp 1 preempt
R3(config-if)#    glbp 1 timers 1 3
R3(config-if)#    glbp 1 ip 192.168.1.150

R3#sh glbp
    FastEthernet0/0 - Group 1
      State is Standby
        1 state change, last state change 00:00:34
      Virtual IP address is 192.168.1.150
      Hello time 1 sec, hold time 3 sec
        Next hello sent in 0.492 secs
      Redirect time 600 sec, forwarder time-out 14400 sec
      Authentication MD5, key-string "cisco"
      Preemption enabled, min delay 0 sec
      Active is 192.168.1.100, priority 120 (expires in 2.556 sec)
      Standby is local
      Priority 100 (default)
      Weighting 100 (default 100), thresholds: lower 1, upper 100
      Load balancing: round-robin
```

```
  Group members:
    cc01.06c4.0000 (192.168.1.100) authenticated
    cc03.06c4.0000 (192.168.1.200) local
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Listen
    MAC address is 0007.b400.0101 (learnt)
    Owner ID is cc01.06c4.0000
    Time to live: 14399.556 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.1.100 (primary), weighting 100 (expires in 2.056 sec)
  Forwarder 2
    State is Active
      1 state change, last state change 00:00:35
    MAC address is 0007.b400.0102 (default)
    Owner ID is cc03.06c4.0000
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
```

```
R3#sh glbp  brief
    Interface   Grp  Fwd Pri State    Address         Active router   Standby router
    Fa0/0       1    -   100 Standby  192.168.1.150   192.168.1.100   local
    Fa0/0       1    1   -   Listen   0007.b400.0101  192.168.1.100   -
    Fa0/0       1    2   -   Active   0007.b400.0102  local           -
```

```
R1#sh glbp
    FastEthernet0/0 - Group 1
      State is Active
        2 state changes, last state change 00:02:33
      Virtual IP address is 192.168.1.150
      Hello time 1 sec, hold time 3 sec
        Next hello sent in 0.512 secs
      Redirect time 600 sec, forwarder time-out 14400 sec
      Authentication MD5, key-string "cisco"
      Preemption enabled, min delay 0 sec
      Active is local
      Standby is 192.168.1.200, priority 100 (expires in 2.436 sec)
      Priority 120 (configured)
      Weighting 100 (default 100), thresholds: lower 1, upper 100
      Load balancing: round-robin
      Group members:
        cc01.06c4.0000 (192.168.1.100) local
        cc03.06c4.0000 (192.168.1.200) authenticated
```

```
There are 2 forwarders (1 active)
Forwarder 1
  State is Active
    1 state change, last state change 00:02:30
  MAC address is 0007.b400.0101 (default)
  Owner ID is cc01.06c4.0000
  Redirection enabled
  Preemption enabled, min delay 30 sec
  Active is local, weighting 100
Forwarder 2
  State is Listen
  MAC address is 0007.b400.0102 (learnt)
  Owner ID is cc03.06c4.0000
  Redirection enabled, 599.772 sec remaining (maximum 600 sec)
  Time to live: 14399.772 sec (maximum 14400 sec)
  Preemption enabled, min delay 30 sec
  Active is 192.168.1.200 (primary), weighting 100 (expires in 2.772 sec)
```

R1#sh glbp brief

```
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Fa0/0       1    -   120 Active   192.168.1.150   local           192.168.1.200
Fa0/0       1    1   -   Active   0007.b400.0101  local           -
Fa0/0       1    2   -   Listen   0007.b400.0102  192.168.1.200   -
```

R5#clear arp-cache

R5#ping 192.168.1.150

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/224/1040 ms
```

R5#sh ip arp

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.2            -   cc05.04dc.0000  ARPA   FastEthernet0/0
Internet  192.168.1.150          0   0007.b400.0101  ARPA   FastEthernet0/0
```

TASK:

- Configure R1 to track interface s1/0
- If the interfaces s1/0 goes down, GLBP has to automatically stop using R1 as AVF.

```
R1(config)#int f0/0
R1(config-if)# glbp 1 weighting track 1   decrement 100
R1(config-if)#exit
```

- Default weighting will be 100 and if the interface goes down, weighting will be decremented to 0
- If weight value equals to 0, the AVF will not be used to forward traffic

TASK:

- Configure R1 to track interface s1/0
- If the interfaces s1/0 goes down, GLBP has to automatically stop using R1 as AVF ..
- Use default weighting (100) and default decrement values (10)

```
R1(config)#int f0/0
R1(config-if)# glbp 1 weighting track 1
R1(config-if)#glbp 1 weighting 100  lower 95
R1(config-if)# glbp 1 weighting track 1 decrement 10
R1(config-if)#exit

R1#sh glbp
    FastEthernet0/0 - Group 1
      State is Active
        4 state changes, last state change 00:30:43
      Virtual IP address is 192.168.1.150
      Hello time 1 sec, hold time 3 sec
        Next hello sent in 0.600 secs
      Redirect time 600 sec, forwarder time-out 14400 sec
      Authentication MD5, key-string "cisco"
      Preemption enabled, min delay 0 sec
      Active is local
      Standby is 192.168.1.200, priority 100 (expires in 2.432 sec)
      Priority 120 (configured)
      Weighting 100 (configured 100), thresholds: lower 95, upper 100
        Track object 1 state Up decrement 10
      Load balancing: round-robin
      Group members:
        cc0b.1c94.0000 (192.168.1.100) local
        cc0d.1c94.0000 (192.168.1.200) authenticated
      There are 2 forwarders (1 active)
      Forwarder 1
        State is Active
          3 state changes, last state change 00:30:14
        MAC address is 0007.b400.0101 (default)
        Owner ID is cc0b.1c94.0000
        Redirection enabled
        Preemption enabled, min delay 30 sec
        Active is local, weighting 100
      Forwarder 2
        State is Listen
        MAC address is 0007.b400.0102 (learnt)
        Owner ID is cc0d.1c94.0000
```

```
        Redirection enabled, 599.152 sec remaining (maximum 600 sec)
        Time to live: 14399.152 sec (maximum 14400 sec)
        Preemption enabled, min delay 30 sec
        Active is 192.168.1.200 (primary), weighting 100 (expires in 2.152 sec)

R1(config)#int s1/0
R1(config-if)#shutdown
R1(config-if)#end

R1#sh glbp
        FastEthernet0/0 - Group 1
          State is Active
            4 state changes, last state change 00:31:12
          Virtual IP address is 192.168.1.150
          Hello time 1 sec, hold time 3 sec
            Next hello sent in 0.420 secs
          Redirect time 600 sec, forwarder time-out 14400 sec
          Authentication MD5, key-string "cisco"
          Preemption enabled, min delay 0 sec
          Active is local
          Standby is 192.168.1.200, priority 100 (expires in 2.220 sec)
          Priority 120 (configured)
          Weighting 90 (configured 100), thresholds: lower 95, upper 100
            Track object 1 state Down decrement 10
          Load balancing: round-robin
          Group members:
            cc0b.1c94.0000 (192.168.1.100) local
            cc0d.1c94.0000 (192.168.1.200) authenticated
          There are 2 forwarders (1 active)
          Forwarder 1
            State is Active
              3 state changes, last state change 00:30:43
            MAC address is 0007.b400.0101 (default)
            Owner ID is cc0b.1c94.0000
            Redirection enabled
            Preemption enabled, min delay 30 sec
            Active is local, weighting 90
          Forwarder 2
            State is Listen
            MAC address is 0007.b400.0102 (learnt)
            Owner ID is cc0d.1c94.0000
            Redirection enabled, 599.152 sec remaining (maximum 600 sec)
            Time to live: 14399.152 sec (maximum 14400 sec)
            Preemption enabled, min delay 30 sec
```

```
        Active is 192.168.1.200 (primary), weighting 100 (expires in 2.152 sec)
    R1#
```

```
R4#traceroute 12.0.0.1
        Type escape sequence to abort.
        Tracing the route to 12.0.0.1

          1 192.168.1.200 64 msec 20 msec 28 msec
          2 2.2.2.1 84 msec
```

```
R5#traceroute 12.0.0.1
        Type escape sequence to abort.
        Tracing the route to 12.0.0.1

          1 192.168.1.200 76 msec 28 msec 32 msec
          2 2.2.2.1 64 msec *  44 msec
```

```
R6#traceroute 12.0.0.1
        Type escape sequence to abort.
        Tracing the route to 12.0.0.1

          1 192.168.1.200 48 msec 40 msec 16 msec
          2 2.2.2.1 104 msec
```

TASK:

- Change the s1/0 interface back to NO Shutdown
- Configure GLBP to perform host-based Load balancing

```
R1(config)#int f0/0
R1(config-if)#  no shutdown
R1(config-if)#end
```

```
R1#sh glbp
    FastEthernet0/0 - Group 1
      State is Active
        6 state changes, last state change 00:05:58
      Virtual IP address is 192.168.1.150
      Hello time 1 sec, hold time 3 sec
        Next hello sent in 0.656 secs
      Redirect time 600 sec, forwarder time-out 14400 sec
      Authentication MD5, key-string "cisco"
      Preemption enabled, min delay 0 sec
      Active is local
      Standby is 192.168.1.200, priority 100 (expires in 2.188 sec)
```

Priority 120 (configured)
Weighting 100 (configured 100), thresholds: lower 95, upper 100
Track object 1 state Up decrement 10
Load balancing: round-robin
Group members:
cc0b.1c94.0000 (192.168.1.100) local
cc0d.1c94.0000 (192.168.1.200) authenticated
There are 2 forwarders (1 active)
Forwarder 1
State is Active
5 state changes, last state change 00:05:29
MAC address is 0007.b400.0101 (default)
Owner ID is cc0b.1c94.0000
Redirection enabled
Preemption enabled, min delay 30 sec
Active is local, weighting 100
Arp replies sent: 5
Forwarder 2
State is Listen
MAC address is 0007.b400.0102 (learnt)
Owner ID is cc0d.1c94.0000
Redirection enabled, 599.436 sec remaining (maximum 600 sec)
Time to live: 14399.436 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 192.168.1.200 (primary), weighting 100 (expires in 2.428 sec)
Arp replies sent: 5

R1/R3

```
R1(config)# int f0/0
R1(config-if)#  glbp 1 load-balancing host-dependent
R1(config-if)#  exit

R1#sh glbp
FastEthernet0/0 - Group 1
  State is Active
    6 state changes, last state change 00:07:05
  Virtual IP address is 192.168.1.150
  Hello time 1 sec, hold time 3 sec
    Next hello sent in 0.496 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Authentication MD5, key-string "cisco"
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 192.168.1.200, priority 100 (expires in 2.792 sec)
  Priority 120 (configured)
```

```
  Weighting 100 (configured 100), thresholds: lower 95, upper 100
    Track object 1 state Up decrement 10
  Load balancing: host-dependent
  Group members:
    cc0b.1c94.0000 (192.168.1.100) local
    cc0d.1c94.0000 (192.168.1.200) authenticated
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      5 state changes, last state change 00:06:36
    MAC address is 0007.b400.0101 (default)
    Owner ID is cc0b.1c94.0000
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
    Arp replies sent: 5
  Forwarder 2
    State is Listen
    MAC address is 0007.b400.0102 (learnt)
    Owner ID is cc0d.1c94.0000
    Redirection enabled, 599.956 sec remaining (maximum 600 sec)
    Time to live: 14399.960 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.1.200 (primary), weighting 100 (expires in 2.952 sec)
    Arp replies sent: 5
```

TASK:

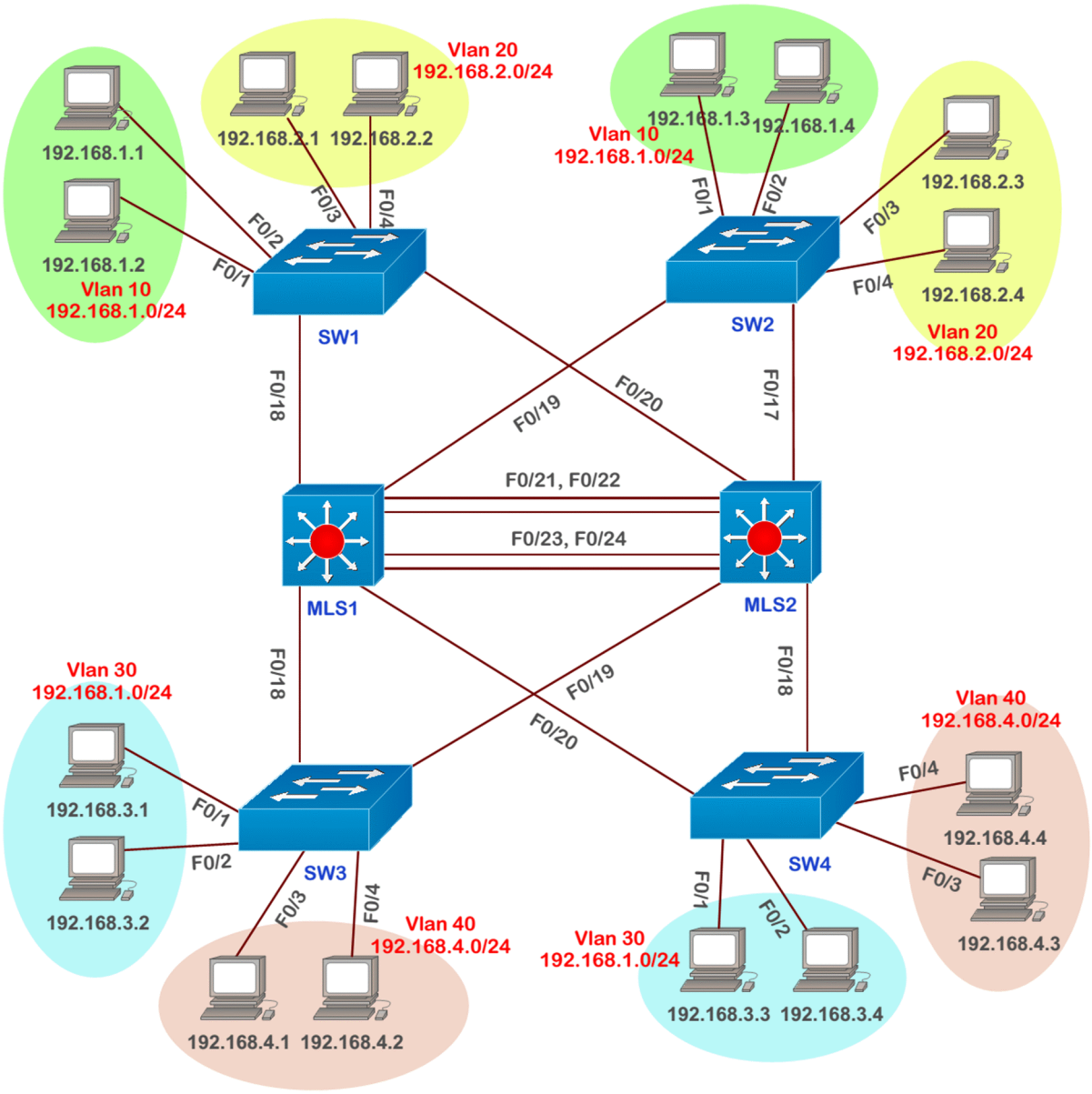
- Configure R1/R3 to do weighted load balancing between Gateways.
- Ensure that R1 forward traffic as AVG with ratio of R1:R3 = 2:1

```
R1(config)#int f0/0
R1(config-if)#glbp 1 load-balancing weighted
R1(config-if)#glbp 1 weighting 100
R1(config-if)#end

R3(config)# int f0/0
R3(config-if)#  glbp 1 load-balancing weighted
R3(config-if)#  glbp 1 weighting 50
R3(config-if)#end

R3#sh glbp
    FastEthernet0/0 - Group 1
      State is Standby
        7 state changes, last state change 00:42:36
      Virtual IP address is 192.168.1.150
```

```
  Hello time 1 sec, hold time 3 sec
    Next hello sent in 0.420 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Authentication MD5, key-string "cisco"
  Preemption enabled, min delay 0 sec
  Active is 192.168.1.100, priority 120 (expires in 2.352 sec)
  Standby is local
  Priority 100 (default)
  Weighting 50 (configured 50), thresholds: lower 1, upper 50
  Load balancing: weighted
  Group members:
    cc0b.1c94.0000 (192.168.1.100) authenticated
    cc0d.1c94.0000 (192.168.1.200) local
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Listen
      4 state changes, last state change 00:42:10
    MAC address is 0007.b400.0101 (learnt)
    Owner ID is cc0b.1c94.0000
    Time to live: 14399.176 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.1.100 (primary), weighting 100 (expires in 2.168 sec)
    Arp replies sent: 2
  Forwarder 2
    State is Active
      1 state change, last state change 02:22:24
    MAC address is 0007.b400.0102 (default)
    Owner ID is cc0d.1c94.0000
    Preemption enabled, min delay 30 sec
    Active is local, weighting 50
    Arp replies sent: 2

R1#sh glbp
  FastEthernet0/0 - Group 1
    State is Active
      6 state changes, last state change 00:48:01
    Virtual IP address is 192.168.1.150
    Hello time 1 sec, hold time 3 sec
      Next hello sent in 0.268 secs
    Redirect time 600 sec, forwarder time-out 14400 sec
    Authentication MD5, key-string "cisco"
    Preemption enabled, min delay 0 sec
    Active is local
    Standby is 192.168.1.200, priority 100 (expires in 2.852 sec)
```

Priority 120 (configured)
Weighting 100 (configured 100), thresholds: lower 95, upper 100
  Track object 1 state Up decrement 10
Load balancing: weighted
Group members:
  cc0b.1c94.0000 (192.168.1.100) local
  cc0d.1c94.0000 (192.168.1.200) authenticated
There are 2 forwarders (1 active)
Forwarder 1
  State is Active
    5 state changes, last state change 00:47:32
  MAC address is 0007.b400.0101 (default)
  Owner ID is cc0b.1c94.0000
  Redirection enabled
  Preemption enabled, min delay 30 sec
  Active is local, weighting 100
  Arp replies sent: 5
Forwarder 2
  State is Listen
  MAC address is 0007.b400.0102 (learnt)
  Owner ID is cc0d.1c94.0000
  Redirection enabled, 599.088 sec remaining (maximum 600 sec)
  Time to live: 14399.088 sec (maximum 14400 sec)
  Preemption enabled, min delay 30 sec
  Active is 192.168.1.200 (primary), weighting 50 (expires in 2.088 sec)
  Arp replies sent: 5

SWITCHING MOCK LAB:



Questions:

Ether Channel:

- Configure the links connecting between MLS1 and MLS2 as logical link using LACP Negotiation process

Trunking

- Configure Trunking on MLS 1 and MLS2 port channel link connecting each other
- Should be configured as Manual Trunk and disable DTP
- Configure the trunk links to carry on the traffic for the VLAN which exists in our network.

VTP

- Configure VTP version 2 on all switches
- MLS1 & MLS2 Must be Server and all the remaining switches must be Clients
    - Domain Name : CCNP

- Password : cisco123
-

- Create Vlan 10 (Accounts), Vlan 20 (marketing) , Vlan 30(Sales), Vlan 40 (HR) and shift ports as per the diagram.

Access Ports

- Connect PC as per the diagram and Use Network as given below
  - VLAN 10 192.168.1.0/24
  - VLAN 20 192.168.2.0/24
  - VLAN 30 192.168.3.0/24
  - VLAN 40 192.168.4.0/24
- Ensure that the users on the same VLAN users can communicate with to each other

Inter-Vlan Routing

- Create SVI on MLS 1 for each Vlan:
  - VLAN 10 192.168.1.100
  - VLAN 20 192.168.2.100
  - VLAN 30 192.168.3.100
  - VLAN 40 192.168.4.100
- Ensure that the different VLAN users can Communicate with to each other

STP

- Find the Root Bridge for all Vlan (10, 20, 30, 40, 1).
- List the Root Ports of every Non Root Bridge.
- List the Alternate (Blocking) Ports present in the topology

Tuning STP

- Configure MLS1 to be the Primary Root Bridge for Vlan 10 & 20 and Backup for Vlan 30 & 40
- Configure MLS2 to be the Primary Root Bridge for Vlan 30 & 40 and Backup for Vlan 10 & 20
- List the Root Ports of every Non Root Bridge.
- List the Alternate (Blocking) Ports present in the topology

Port Security

- Configure Port Security on MLS1 f0/10
- Configure f0/10 as access port and in vlan 10
- Configure Maximum Mac-address limit to 3 if exceeds the port has to shutdown automatically.

Solutions:

TASK: Ether Channel:

- Configure the links connecting between MLS1 and MLS2 as logical link using LACP Negotiation process

```
MLS-1(config)#int range f0/21 - 24
MLS-1(config-if-range)#channel-group 12 ?
      mode  Etherchannel Mode of the interface

MLS-1(config-if-range)#channel-group 12 mode ?
      active     Enable LACP unconditionally
      auto       Enable PAgP only if a PAgP device is detected
      desirable  Enable PAgP unconditionally
      on         Enable Etherchannel only
```

passive Enable LACP only if a LACP device is detected

MLS-1(config-if-range)#channel-group 12 mode active
MLS-1(config-if-range)#end

MLS-2(config)#int range f0/21 - 24
MLS-2(config-if-range)#channel-group 12 mode passive
MLS-2(config-if-range)#end

MLS-2#sh etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+---
12 Po12(SU) LACP Fa0/21(P) Fa0/22(P) Fa0/23(P) Fa0/24(P)

MLS-2#sh ip int brief
Port-channel 12 unassigned YES unset up up

MLS-1#sh etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+---
12 Po12(SU) LACP Fa0/21(P) Fa0/22(P) Fa0/23(P) Fa0/24(P)

TASK: Trunking

- Configure Trunking on MLS 1 and MLS2 port channel link connecting each other
- Should be configured as Manual Trunk and disable DTP
- Configure the trunk links to carry on the traffic for the VLAN which exists in our network.

On Both MLS1 and MLS2

```
MLS-2(config)# int port-channel 12
MLS-2(config-if)#  switchport trunk encapsulation dot1q
MLS-2(config-if)#  switchport mode trunk
MLS-2(config-if)#switchport nonegotiate
MLS-2(config-if)#switchport trunk allowed vlan 10,20,30,40
MLS-2(config-if)#  end
```

```
MLS-1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po12        on           802.1q         trunking      1
Port        Vlans allowed on trunk
Po12        10,20,30,40
Port        Vlans allowed and active in management domain
Po12        none
Port        Vlans in spanning tree forwarding state and not pruned
Po12        none
```

```
MLS-2#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po12        on           802.1q         trunking      1

Port        Vlans allowed on trunk
Po12        10,20,30,40

Port        Vlans allowed and active in management domain
Po12        none

Port        Vlans in spanning tree forwarding state and not pruned
Po12        none
```

MLS 1 and MLS-2

```
MLS-1(config)#int range f0/17 - 20
MLS-1(config-if-range)#  switchport trunk encapsulation dot1q
MLS-1(config-if-range)#  switchport mode trunk
MLS-1(config-if-range)#  switchport nonegotiate
MLS-1(config-if-range)#  switchport trunk allowed vlan 10,20,30,40
MLS-1(config-if-range)# end
```

MLS-2#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/17	on	802.1q	trunking	1
Fa0/18	on	802.1q	trunking	1
Fa0/19	on	802.1q	trunking	1
Fa0/20	on	802.1q	trunking	1
Po12	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/17	10,20,30,40
Fa0/18	10,20,30,40
Fa0/19	10,20,30,40
Fa0/20	10,20,30,40
Po12	10,20,30,40

Port	Vlans allowed and active in management domain
Fa0/17	none
Fa0/18	none
Fa0/19	none
Fa0/20	none
Po12	none

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/17	none
Fa0/18	none
Fa0/19	none
Fa0/20	none
Po12	none

MLS-1#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/17	on	802.1q	trunking	1
Fa0/18	on	802.1q	trunking	1
Fa0/19	on	802.1q	trunking	1
Fa0/20	on	802.1q	trunking	1
Po12	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/17	10,20,30,40
Fa0/18	10,20,30,40
Fa0/19	10,20,30,40
Fa0/20	10,20,30,40
Po12	10,20,30,40

```
Port        Vlans allowed and active in management domain
Fa0/17      none
Fa0/18      none
Fa0/19      none
Fa0/20      none
Po12        none

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/17      none
Fa0/18      none
Fa0/19      none
Fa0/20      none
Po12        none
```

SW1/SW2

```
SW-1(config)#int range f0/17, f0/19
SW-1(config-if-range)#  switchport mode trunk
SW-1(config-if-range)#  switchport trunk encapsulation dot1q
SW-1(config-if-range)#  switchport nonegotiate
SW-1(config-if-range)#  switchport trunk allowed vlan 10,20,30,40
SW-1(config-if-range)#  end
```

```
SW-2#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/17      on           802.1q         trunking      1
Fa0/19      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/17      10,20,30,40
Fa0/19      10,20,30,40

Port        Vlans allowed and active in management domain
Fa0/17      none
Fa0/19      none

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/17      none
Fa0/19      none
```

```
SW-1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/17      on           802.1q         trunking      1
Fa0/19      on           802.1q         trunking      1
```

```
Port        Vlans allowed on trunk
Fa0/17      10,20,30,40
Fa0/19      10,20,30,40

Port        Vlans allowed and active in management domain
Fa0/17      none
Fa0/19      none

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/17      none
Fa0/19      none
```

SW3/SW4

```
SW-3(config)#int range f0/18, f0/20
SW-3(config-if-range)#  switchport mode trunk
SW-3(config-if-range)#  switchport trunk encapsulation dot1q
SW-3(config-if-range)#  switchport nonegotiate
SW-3(config-if-range)#  switchport trunk allowed vlan 10,20,30,40
SW-3(config-if-range)#  end
SW-4#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/18      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/18      10,20,30,40
Fa0/20      10,20,30,40

Port        Vlans allowed and active in management domain
Fa0/18      none
Fa0/20      none

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/18      none
Fa0/20      none

SW-3#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/18      on           802.1q         trunking      1
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/18      10,20,30,40
```

Fa0/20 10,20,30,40

Port Vlans allowed and active in management domain
Fa0/18 none
Fa0/20 none

Port Vlans in spanning tree forwarding state and not pruned
Fa0/18 none
Fa0/20 none

TASK: VTP

- Configure VTP version 2 on all switches
- MLS1 & MLS2 Must be Server and all the remaining switches must be Clients
  - Domain Name : CCNP
  - Password : cisco123
- Create Vlan 10 (Accounts), Vlan 20 (marketing) , Vlan 30(Sales), Vlan 40 (HR) and shift ports as per the diagram.

On MLS-1 & MLS-2

```
MLS-x(config)# vtp domain CCNP
MLS-x(config)#  vtp password cisco123
MLS-x(config)#  vtp mode server
MLS-x(config)#  vtp version 2
```

MLS-2#sh vtp status

```
VTP Version                     : 2
Configuration Revision          : 3
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8F 0xD0 0xDD 0x26 0xCD 0x77 0xC9 0x39
Configuration last modified by 0.0.0.0 at 3-1-93 00:37:11
Local updater ID is 0.0.0.0 (no valid interface found)
```

MLS-1#sh vtp status

```
VTP Version                     : 2
Configuration Revision          : 3
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Server
```

```
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8F 0xD0 0xDD 0x26 0xCD 0x77 0xC9 0x39
Configuration last modified by 0.0.0.0 at 3-1-93 00:37:11
Local updater ID is 0.0.0.0 (no valid interface found)
```

SW1/SW2/SW3/SW4

```
SW-1(config)#vtp domain CCNP
SW-1(config)#vtp password cisco123
SW-1(config)#vtp version 2
SW-1(config)#vtp mode client
SW-1(config)#end
```

```
SW-1#sh vtp status
    VTP Version                     : 2
    Configuration Revision          : 3
    Maximum VLANs supported locally : 255
    Number of existing VLANs        : 5
    VTP Operating Mode              : Client
    VTP Domain Name                 : CCNP
    VTP Pruning Mode                : Disabled
    VTP V2 Mode                     : Enabled
    VTP Traps Generation            : Disabled
    MD5 digest                      : 0x8F 0xD0 0xDD 0x26 0xCD 0x77 0xC9 0x39
    Configuration last modified by 0.0.0.0 at 3-1-93 00:37:11
```

```
SW-4#sh vtp status
    VTP Version                     : 2
    Configuration Revision          : 3
    Maximum VLANs supported locally : 255
    Number of existing VLANs        : 5
    VTP Operating Mode              : Client
    VTP Domain Name                 : CCNP
    VTP Pruning Mode                : Disabled
    VTP V2 Mode                     : Enabled
    VTP Traps Generation            : Disabled
    MD5 digest                      : 0x8F 0xD0 0xDD 0x26 0xCD 0x77 0xC9 0x39
    Configuration last modified by 0.0.0.0 at 3-1-93 00:37:11
```

```
MLS-1(config)#vlan 10
MLS-1(config-vlan)#name Accounts
```

```
MLS-1(config-vlan)#vlan 20
MLS-1(config-vlan)#name Marketing
MLS-1(config-vlan)#vlan 30
MLS-1(config-vlan)#name Sales
MLS-1(config-vlan)#vlan 40
MLS-1(config-vlan)#name HR
MLS-1(config-vlan)#exit

MLS-1#sh vlan
    VLAN Name                             Status    Ports
    ---- -------------------------------- --------- -------------------------------
    1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                    Gig0/1, Gig0/2
    10   Accounts                         active
    20   Marketing                        active
    30   Sales                            active
    40   HR                               active
    1002 fddi-default                     act/unsup
    1003 token-ring-default               act/unsup
    1004 fddinet-default                  act/unsup
    1005 trnet-default                    act/unsup

MLS-1#sh vtp status
    VTP Version              : 2
    Configuration Revision   : 11
    Maximum VLANs supported locally : 1005
    Number of existing VLANs : 9
    VTP Operating Mode       : Server
    VTP Domain Name          : CCNP
    VTP Pruning Mode         : Disabled
    VTP V2 Mode              : Enabled
    VTP Traps Generation     : Disabled
    MD5 digest               : 0xD3 0x30 0x49 0xF1 0x6D 0x80 0x74 0x90
    Configuration last modified by 0.0.0.0 at 3-1-93 00:40:40
    Local updater ID is 0.0.0.0 (no valid interface found)

MLS-2#sh vtp status
    VTP Version              : 2
    Configuration Revision   : 11
    Maximum VLANs supported locally : 1005
    Number of existing VLANs : 9
```

VTP Operating Mode : Server
VTP Domain Name : CCNP
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0xD3 0x30 0x49 0xF1 0x6D 0x80 0x74 0x90
Configuration last modified by 0.0.0.0 at 3-1-93 00:40:40
Local updater ID is 0.0.0.0 (no valid interface found)

MLS-2#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
			Fa0/5, Fa0/6, Fa0/7, Fa0/8
			Fa0/9, Fa0/10, Fa0/11, Fa0/12
			Fa0/13, Fa0/14, Fa0/15, Fa0/16
			Gig0/1, Gig0/2
10	Accounts	active	
20	Marketing	active	
30	Sales	active	
40	HR	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

SW-1#sh vtp status
VTP Version : 2
Configuration Revision : 11
Maximum VLANs supported locally : 255
Number of existing VLANs : 9
VTP Operating Mode : Client
VTP Domain Name : CCNP
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0xD3 0x30 0x49 0xF1 0x6D 0x80 0x74 0x90
Configuration last modified by 0.0.0.0 at 3-1-93 00:40:40

SW-1#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
			Fa0/5, Fa0/6, Fa0/7, Fa0/8

```
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/18, Fa0/20, Fa0/21, Fa0/22
                                    Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   Accounts                       active
20   Marketing                      active
30   Sales                          active
40   HR                             active
1002 fddi-default                   act/unsup
1003 token-ring-default             act/unsup
1004 fddinet-default                act/unsup
1005 trnet-default                  act/unsup
```

SW-2#sh vlan

```
VLAN Name                           Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/18, Fa0/20, Fa0/21, Fa0/22
                                    Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   Accounts                       active
20   Marketing                      active
30   Sales                          active
40   HR                             active
1002 fddi-default                   act/unsup
1003 token-ring-default             act/unsup
```

SW-3#sh vlan

```
VLAN Name                           Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/19, Fa0/21, Fa0/22
                                    Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   Accounts                       active
20   Marketing                      active
30   Sales                          active
40   HR                             active
1002 fddi-default                   act/unsup
1003 token-ring-default             act/unsup
```

```
1004 fddinet-default                act/unsup
1005 trnet-default                  act/unsup
```

```
SW-4#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/19, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   Accounts                          active
20   Marketing                         active
30   Sales                             active
40   HR                                active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

```
SW-1(config)#int range f0/1 - 2
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 10
SW-1(config-if-range)#exit

SW-1(config)#int range f0/3 - 4
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 20
SW-1(config-if-range)#exit
```

```
SW-1#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/18, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   Accounts                          active    Fa0/1, Fa0/2
20   Marketing                         active    Fa0/3, Fa0/4
30   Sales                             active
40   HR                                active
```

```
SW-2(config)# int range f0/1 - 2
SW-2(config-if-range)#  switchport mode access
SW-2(config-if-range)#  switchport access vlan 10
SW-2(config-if-range)#  exit

SW-2(config)#  int range f0/3 - 4
SW-2(config-if-range)#  switchport mode access
SW-2(config-if-range)#  switchport access vlan 20
SW-2(config-if-range)#  exit
SW-2(config)#  end

SW-2#sh vlan
    VLAN Name                              Status    Ports
    ---- --------------------------------- --------- -------------------------------
    1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                     Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                     Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                     Fa0/18, Fa0/20, Fa0/21, Fa0/22
                                                     Fa0/23, Fa0/24, Gig1/1, Gig1/2
    10   Accounts                          active    Fa0/1, Fa0/2
    20   Marketing                         active    Fa0/3, Fa0/4
    30   Sales                             active
    40   HR                                active
    1002 fddi-default                      act/unsup
    1003 token-ring-default                act/unsup
    1004 fddinet-default                   act/unsup
    1005 trnet-default                     act/unsup
SW-3(config)# int range f0/1 - 2
SW-3(config-if-range)#  switchport mode access
SW-3(config-if-range)#  switchport access vlan 30
SW-3(config-if-range)#  exit

SW-3(config)#  int range f0/3 - 4
SW-3(config-if-range)#  switchport mode access
SW-3(config-if-range)#  switchport access vlan 40
SW-3(config-if-range)#  end

SW-3#sh vlan
    VLAN Name                              Status    Ports
    ---- --------------------------------- --------- -------------------------------
    1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                     Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                     Fa0/13, Fa0/14, Fa0/15, Fa0/16
```

```
                                    Fa0/17, Fa0/19, Fa0/21, Fa0/22
                                    Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   Accounts                     active
20   Marketing                    active
30   Sales                        active    Fa0/1, Fa0/2
40   HR                           active    Fa0/3, Fa0/4
1002 fddi-default                 act/unsup
1003 token-ring-default           act/unsup
1004 fddinet-default              act/unsup
1005 trnet-default                act/unsup
```

```
SW-4(config)# int range f0/1 - 2
SW-4(config-if-range)#  switchport mode access
SW-4(config-if-range)#  switchport access vlan 30
SW-4(config-if-range)#  exit

SW-4(config)#  int range f0/3 - 4
SW-4(config-if-range)#  switchport mode access
SW-4(config-if-range)#  switchport access vlan 40
SW-4(config-if-range)#  exit
SW-4(config)#end
SW-4#sh vlan
VLAN Name                         Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                      active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/19, Fa0/21, Fa0/22
                                    Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   Accounts                     active
20   Marketing                    active
30   Sales                        active    Fa0/1, Fa0/2
40   HR                           active    Fa0/3, Fa0/4
1002 fddi-default                 act/unsup
1003 token-ring-default           act/unsup
1004 fddinet-default              act/unsup
1005 trnet-default                act/unsup
```

TASK:

- Connect PC as per the diagram and Use Network as given below
  - VLAN 10 192.168.1.0/24
  - VLAN 20 192.168.2.0/24
  - VLAN 30 192.168.3.0/24
  - VLAN 40 192.168.4.0/24
- Ensure that the users on the same VLAN users can communicate with to each other

PC>ipconfig

FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::290:21FF:FEC5:A242
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=51ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 51ms, Average = 13ms

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=27ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=54ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 54ms, Average = 20ms

PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=21ms TTL=128
Reply from 192.168.1.4: bytes=32 time=47ms TTL=128
Reply from 192.168.1.4: bytes=32 time=2ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 47ms, Average = 17ms

PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::230:F2FF:FE6D:DA13
IP Address.....: 192.168.2.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.100
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=10ms TTL=128
Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
Reply from 192.168.2.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 3ms

PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=15ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.2.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 15ms, Average = 3ms

PC>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=22ms TTL=128
Reply from 192.168.2.4: bytes=32 time=0ms TTL=128
Reply from 192.168.2.4: bytes=32 time=0ms TTL=128

Reply from 192.168.2.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.2.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 22ms, Average = 5ms

PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::260:3EFF:FE03:81A4
IP Address.....: 192.168.3.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.3.100

PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=1ms TTL=128
Reply from 192.168.3.2: bytes=32 time=1ms TTL=128
Reply from 192.168.3.2: bytes=32 time=0ms TTL=128
Reply from 192.168.3.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.3.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=104ms TTL=128
Reply from 192.168.3.3: bytes=32 time=0ms TTL=128
Reply from 192.168.3.3: bytes=32 time=0ms TTL=128
Reply from 192.168.3.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 104ms, Average = 26ms

PC>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time=14ms TTL=128
Reply from 192.168.3.4: bytes=32 time=0ms TTL=128
Reply from 192.168.3.4: bytes=32 time=0ms TTL=128
Reply from 192.168.3.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.3.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 14ms, Average = 3ms

PC>ipconfig

FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::207:ECFF:FE29:E6EB
IP Address.....: 192.168.4.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.4.100

PC>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=1ms TTL=128
Reply from 192.168.4.2: bytes=32 time=0ms TTL=128
Reply from 192.168.4.2: bytes=32 time=0ms TTL=128
Reply from 192.168.4.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.4.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.4.3

Pinging 192.168.4.3 with 32 bytes of data:

Reply from 192.168.4.3: bytes=32 time=14ms TTL=128
Reply from 192.168.4.3: bytes=32 time=44ms TTL=128
Reply from 192.168.4.3: bytes=32 time=0ms TTL=128
Reply from 192.168.4.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.4.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 44ms, Average = 14ms

PC>ping 192.168.4.4

Pinging 192.168.4.4 with 32 bytes of data:

Reply from 192.168.4.4: bytes=32 time=21ms TTL=128
Reply from 192.168.4.4: bytes=32 time=0ms TTL=128
Reply from 192.168.4.4: bytes=32 time=0ms TTL=128
Reply from 192.168.4.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.4.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 21ms, Average = 5ms

TASK:

- Create SVI on MLS 1 for each Vlan:
  - VLAN 10 192.168.1.100
  - VLAN 20 192.168.2.100
  - VLAN 30 192.168.3.100
  - VLAN 40 192.168.4.100
- Ensure that the different VLAN users can Communicate with to each other

MLS-1(config)#int vlan 10
MLS-1(config-if)#ip address 192.168.1.100 255.255.255.0
MLS-1(config-if)#no shutdown
MLS-1(config-if)#exit

MLS-1(config)#int vlan 20
MLS-1(config-if)#ip address 192.168.2.100 255.255.255.0
MLS-1(config-if)#no shutdown
MLS-1(config-if)#exit

MLS-1(config)#int vlan 30
MLS-1(config-if)#ip address 192.168.3.100 255.255.255.0
MLS-1(config-if)#no shutdown
MLS-1(config-if)#exit

MLS-1(config)#int vlan 40
MLS-1(config-if)#ip address 192.168.4.100 255.255.255.0
MLS-1(config-if)#no shutdown
MLS-1(config-if)#end

MLS-1#sh ip int brief

FastEthernet0/17	unassigned	YES unset	up	up
FastEthernet0/18	unassigned	YES unset	up	up
FastEthernet0/19	unassigned	YES unset	up	up
FastEthernet0/20	unassigned	YES unset	up	up
FastEthernet0/21	unassigned	YES unset	up	up
FastEthernet0/22	unassigned	YES unset	up	up
FastEthernet0/23	unassigned	YES unset	up	up
FastEthernet0/24	unassigned	YES unset	up	up
GigabitEthernet0/1	unassigned	YES unset	down	down
GigabitEthernet0/2	unassigned	YES unset	down	down
Vlan1	unassigned	YES unset	administratively down	down
Vlan10	192.168.1.100	YES manual	up	up
Vlan20	192.168.2.100	YES manual	up	up
Vlan30	192.168.3.100	YES manual	up	up
Vlan40	192.168.4.100	YES manual	up	up
Port-channel 12	unassigned	YES unset	up	up

MLS-1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

MLS-1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms

MLS-1#ping 192.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

MLS-1#ping 192.168.4.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

PC>ipconfig

FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::290:21FF:FEC5:A242
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

MLS-1(config)#ip routing

PC>ipconfig

FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::290:21FF:FEC5:A242
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=127
Reply from 192.168.2.1: bytes=32 time=0ms TTL=127
Reply from 192.168.2.1: bytes=32 time=0ms TTL=127
Reply from 192.168.2.1: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 1ms

PC>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=23ms TTL=127

Reply from 192.168.3.1: bytes=32 time=0ms TTL=127
Reply from 192.168.3.1: bytes=32 time=12ms TTL=127
Reply from 192.168.3.1: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.3.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 23ms, Average = 9ms

PC>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 192.168.4.1: bytes=32 time=26ms TTL=127
Reply from 192.168.4.1: bytes=32 time=0ms TTL=127
Reply from 192.168.4.1: bytes=32 time=90ms TTL=127
Reply from 192.168.4.1: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.4.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 90ms, Average = 29ms

TASK: STP

- Find the Root Bridge for all Vlan (10, 20, 30, 40, 1).
- List the Root Ports of every Non Root Bridge.
- List the Alternate (Blocking) Ports present in the topology

MLS-1#sh spanning-tree vlan 10
VLAN0010
Spanning tree enabled protocol ieee
Root ID Priority 32778
Address 0001.C7B5.C137
Cost 19
Port 17(FastEthernet0/17)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 0006.2AC0.46C3
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type

```
Fa0/17          Root FWD 19       128.17   P2p
Fa0/18          Desg FWD 19       128.18   P2p
Fa0/19          Desg FWD 19       128.19   P2p
Fa0/20          Desg FWD 19       128.20   P2p
Fa0/21          Desg FWD 19       128.21   P2p
Fa0/22          Desg FWD 19       128.22   P2p
Fa0/23          Desg FWD 19       128.23   P2p
Fa0/24          Desg FWD 19       128.24   P2p
Po12            Desg FWD 7        128.27   Shr
```

MLS-1#sh spanning-tree vlan 20

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    32788
              Address     0001.C7B5.C137
              Cost        19
              Port        17(FastEthernet0/17)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0006.2AC0.46C3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/17           Root FWD 19        128.17   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p
Po12             Desg FWD 7         128.27   Shr
```

MLS-1#sh cdp neighbors

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID     Local Intrfce   Holdtme    Capability  Platform    Port ID
MLS-2         Por 12          131             3560       Fas 0/24
MLS-2         Por 12          131             3560       Fas 0/22
MLS-2         Por 12          131             3560       Por 12
MLS-2         Por 12          131             3560       Fas 0/21
```

```
MLS-2       Por 12       131          3560      Fas 0/23
SW-1        Fas 0/17     133      S   2960      Fas 0/17
SW-2        Fas 0/19     133      S   2960      Fas 0/19
SW-3        Fas 0/18     133      S   2960      Fas 0/18
SW-4        Fas 0/20     133      S   2960      Fas 0/20
```

SW-1#sh spanning-tree vlan 10

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.C7B5.C137
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0001.C7B5.C137
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/19           Desg FWD 19        128.19   P2p
```

SW-2#sh spanning-tree vlan 10

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.C7B5.C137
             Cost        38
             Port        19(FastEthernet0/19)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00E0.B0AC.210D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

```
Fa0/17           Altn BLK 19       128.17   P2p
Fa0/19           Root FWD 19       128.19   P2p
```

MLS-2#sh spanning-tree vlan 10

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.C7B5.C137
             Cost        19
             Port        19(FastEthernet0/19)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00E0.B034.7088
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po12             Altn BLK 7         128.27   Shr
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Fa0/19           Root FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p
```

SW-2#sh spanning-tree vlan 10

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.C7B5.C137
             Cost        38
             Port        19(FastEthernet0/19)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00E0.B0AC.210D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
```

```
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/17           Altn BLK 19        128.17   P2p
Fa0/19           Root FWD 19        128.19   P2p

SW-3#sh spanning-tree vlan 10
    VLAN0010
      Spanning tree enabled protocol ieee
      Root ID     Priority    32778

    Address     0001.C7B5.C137
                Cost        38
                Port        18(FastEthernet0/18)
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
                Address     0030.F232.71C5
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/18           Root FWD 19        128.18   P2p
    Fa0/20           Altn BLK 19        128.20   P2p

SW-4#sh spanning-tree vlan 10
    VLAN0010
      Spanning tree enabled protocol ieee
      Root ID     Priority    32778
                Address     0001.C7B5.C137
                Cost        38
                Port        20(FastEthernet0/20)
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
                Address     0003.E480.75E6
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/18           Altn BLK 19        128.18   P2p
    Fa0/20           Root FWD 19        128.20   P2p
```

- Alternate Ports and Root ports, Designated ports will be same for all vlan (10,20,30,40)
- As we have one common Root Bridge (SW-1in my example) for all Vlans
- You can verify any way if required for other vlans also..in the above I have listed output of vlan 10 only

TASK:

- Configure MLS1 to be the Primary Root Bridge for Vlan 10 & 20 and Backup for Vlan 30 & 40
- Configure MLS2 to be the Primary Root Bridge for Vlan 30 & 40 and Backup for Vlan 10 & 20

```
MLS-1(config)#spanning-tree vlan 10,20 root primary
MLS-1(config)#spanning-tree vlan 30,40 root secondary
MLS-1(config)#end

MLS-2(config)#spanning-tree vlan 30,40 root primary
MLS-2(config)#spanning-tree vlan 10,20 root secondary
MLS-2(config)#end

MLS-1#sh spanning-tree vlan 10
    VLAN0010
      Spanning tree enabled protocol ieee
      Root ID    Priority    24586
                 Address     0006.2AC0.46C3
                 This bridge is the root
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
                 Address     0006.2AC0.46C3
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                 Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/17           Desg FWD 19        128.17   P2p
    Fa0/18           Desg FWD 19        128.18   P2p
    Fa0/19           Desg FWD 19        128.19   P2p
    Fa0/20           Desg FWD 19        128.20   P2p
    Fa0/21           Desg FWD 19        128.21   P2p
    Fa0/22           Desg FWD 19        128.22   P2p
    Fa0/23           Desg FWD 19        128.23   P2p
    Fa0/24           Desg FWD 19        128.24   P2p
    Po12             Desg FWD 7         128.27   Shr

MLS-1#sh spanning-tree vlan 20
    VLAN0020
      Spanning tree enabled protocol ieee
```

```
  Root ID    Priority    24596
             Address     0006.2AC0.46C3
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596  (priority 24576 sys-id-ext 20)
             Address     0006.2AC0.46C3
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p
Po12             Desg FWD 7         128.27   Shr

MLS-1#sh spanning-tree vlan 30
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    24606
             Address     00E0.B034.7088
             Cost        7
             Port        27(Port-channel 12)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28702  (priority 28672 sys-id-ext 30)
             Address     0006.2AC0.46C3
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
```

```
Fa0/23           Desg FWD 19       128.23   P2p
Fa0/24           Desg FWD 19       128.24   P2p
Po12             Root FWD 7        128.27   Shr
```

MLS-1#sh spanning-tree vlan 40

```
VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    24616
             Address     00E0.B034.7088
             Cost        7
             Port        27(Port-channel 12)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28712  (priority 28672 sys-id-ext 40)
             Address     0006.2AC0.46C3
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p
Po12             Root FWD 7         128.27   Shr
```

MLS-2#sh spanning-tree vlan 30

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    24606
             Address     00E0.B034.7088
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24606  (priority 24576 sys-id-ext 30)
             Address     00E0.B034.7088
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
```

```
---------------- ---- --- --------- -------- --------------------------------
Po12             Desg FWD 7        128.27   Shr
Fa0/17           Desg FWD 19       128.17   P2p
Fa0/18           Desg FWD 19       128.18   P2p
Fa0/19           Desg FWD 19       128.19   P2p
Fa0/20           Desg FWD 19       128.20   P2p
Fa0/21           Desg FWD 19       128.21   P2p
Fa0/22           Desg FWD 19       128.22   P2p
Fa0/23           Desg FWD 19       128.23   P2p
Fa0/24           Desg FWD 19       128.24   P2p
```

MLS-2#sh spanning-tree vlan 40

```
VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    24616
             Address     00E0.B034.7088
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24616  (priority 24576 sys-id-ext 40)
             Address     00E0.B034.7088
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po12             Desg FWD 7        128.27   Shr
Fa0/17           Desg FWD 19       128.17   P2p
Fa0/18           Desg FWD 19       128.18   P2p
Fa0/19           Desg FWD 19       128.19   P2p
Fa0/20           Desg FWD 19       128.20   P2p
Fa0/21           Desg FWD 19       128.21   P2p
Fa0/22           Desg FWD 19       128.22   P2p
Fa0/23           Desg FWD 19       128.23   P2p
Fa0/24           Desg FWD 19       128.24   P2p
```

MLS-2#sh spanning-tree vlan 10

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0006.2AC0.46C3
             Cost        7
             Port        27(Port-channel 12)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    28682  (priority 28672 sys-id-ext 10)
             Address     00E0.B034.7088
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po12             Root FWD 7         128.27   Shr
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p

MLS-2#sh spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address     0006.2AC0.46C3
             Cost        7
             Port        27(Port-channel 12)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     00E0.B034.7088
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po12             Root FWD 7         128.27   Shr
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p
```

```
SW-1#sh spanning-tree vlan 10
    VLAN0010
      Spanning tree enabled protocol ieee
      Root ID    Priority    24586
                 Address     0006.2AC0.46C3
                 Cost        19
                 Port        17(FastEthernet0/17)
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
                 Address     0001.C7B5.C137
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                 Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/2            Desg FWD 19        128.2    P2p
    Fa0/1            Desg FWD 19        128.1    P2p
    Fa0/17           Root FWD 19        128.17   P2p
    Fa0/19           Altn BLK 19        128.19   P2p

    SW-1#sh spanning-tree vlan 20
    VLAN0020
      Spanning tree enabled protocol ieee
      Root ID    Priority    24596
                 Address     0006.2AC0.46C3
                 Cost        19
                 Port        17(FastEthernet0/17)
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
                 Address     0001.C7B5.C137
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                 Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/3            Desg FWD 19        128.3    P2p
    Fa0/4            Desg FWD 19        128.4    P2p
    Fa0/17           Root FWD 19        128.17   P2p
    Fa0/19           Altn BLK 19        128.19   P2p

SW-1#sh spanning-tree vlan 30
    VLAN0030
```

```
  Spanning tree enabled protocol ieee
  Root ID    Priority    24606
             Address     00E0.B034.7088
             Cost        19
             Port        19(FastEthernet0/19)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     0001.C7B5.C137
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/17           Altn BLK 19        128.17   P2p
Fa0/19           Root FWD 19        128.19   P2p
```

SW-1#sh spanning-tree vlan 40

```
VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    24616
             Address     00E0.B034.7088
             Cost        19
             Port        19(FastEthernet0/19)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32808  (priority 32768 sys-id-ext 40)
             Address     0001.C7B5.C137
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/17           Altn BLK 19        128.17   P2p
Fa0/19           Root FWD 19        128.19   P2p
```

SW-2#sh spanning-tree vlan 10

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0006.2AC0.46C3
             Cost        19
             Port        19(FastEthernet0/19)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00E0.B0AC.210D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/17           Altn BLK 19        128.17   P2p
Fa0/19           Root FWD 19        128.19   P2p
```

SW-2#sh spanning-tree vlan 20

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address     0006.2AC0.46C3
             Cost        19
             Port        19(FastEthernet0/19)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     00E0.B0AC.210D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/17           Altn BLK 19        128.17   P2p
Fa0/19           Root FWD 19        128.19   P2p
```

SW-2#sh spanning-tree vlan 30

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    24606
             Address     00E0.B034.7088
             Cost        19
             Port        17(FastEthernet0/17)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
```

```
            Address     00E0.B0AC.210D
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/17           Root FWD 19        128.17   P2p
    Fa0/19           Altn BLK 19        128.19   P2p

SW-2#sh spanning-tree vlan 40
    VLAN0040
      Spanning tree enabled protocol ieee
      Root ID    Priority    24616
            Address     00E0.B034.7088
            Cost        19
            Port        17(FastEthernet0/17)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32808  (priority 32768 sys-id-ext 40)
            Address     00E0.B0AC.210D
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/17           Root FWD 19        128.17   P2p
    Fa0/19           Altn BLK 19        128.19   P2p

SW-3#sh spanning-tree vlan 10
    VLAN0010
      Spanning tree enabled protocol ieee
      Root ID    Priority    24586
            Address     0006.2AC0.46C3
            Cost        19
            Port        18(FastEthernet0/18)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
            Address     0030.F232.71C5
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
```

```
Fa0/18          Root FWD 19       128.18   P2p
Fa0/20          Altn BLK 19       128.20   P2p

SW-3#sh spanning-tree vlan 20
    VLAN0020
      Spanning tree enabled protocol ieee
      Root ID    Priority    24596
                 Address     0006.2AC0.46C3
                 Cost        19
                 Port        18(FastEthernet0/18)
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
                 Address     0030.F232.71C5
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                 Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/18           Root FWD 19        128.18   P2p
    Fa0/20           Altn BLK 19        128.20   P2p

SW-3#sh spanning-tree vlan 30
    VLAN0030
      Spanning tree enabled protocol ieee
      Root ID    Priority    24606
                 Address     00E0.B034.7088
                 Cost        19
                 Port        20(FastEthernet0/20)
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
                 Address     0030.F232.71C5
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                 Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/1            Desg FWD 19        128.1    P2p
    Fa0/2            Desg FWD 19        128.2    P2p
    Fa0/18           Altn BLK 19        128.18   P2p
    Fa0/20           Root FWD 19        128.20   P2p

SW-3#sh spanning-tree vlan 40
```

```
VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    24616
             Address     00E0.B034.7088
             Cost        19
             Port        20(FastEthernet0/20)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32808  (priority 32768 sys-id-ext 40)
             Address     0030.F232.71C5
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/18           Altn BLK 19        128.18   P2p
Fa0/20           Root FWD 19        128.20   P2p

SW-4#sh spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0006.2AC0.46C3
             Cost        19
             Port        20(FastEthernet0/20)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0003.E480.75E6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/18           Altn BLK 19        128.18   P2p
Fa0/20           Root FWD 19        128.20   P2p

SW-4#sh spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address     0006.2AC0.46C3
```

```
              Cost        19
              Port        20(FastEthernet0/20)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0003.E480.75E6
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/18           Altn BLK 19        128.18   P2p
    Fa0/20           Root FWD 19        128.20   P2p

SW-4#sh spanning-tree vlan 30
    VLAN0030
      Spanning tree enabled protocol ieee
      Root ID    Priority    24606
              Address     00E0.B034.7088
              Cost        19
              Port        18(FastEthernet0/18)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

      Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
              Address     0003.E480.75E6
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/1            Desg FWD 19        128.1    P2p
    Fa0/2            Desg FWD 19        128.2    P2p
    Fa0/18           Root FWD 19        128.18   P2p
    Fa0/20           Altn BLK 19        128.20   P2p

SW-4#sh spanning-tree vlan 40
    VLAN0040
      Spanning tree enabled protocol ieee
      Root ID    Priority    24616
              Address     00E0.B034.7088
              Cost        19
              Port        18(FastEthernet0/18)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    32808  (priority 32768 sys-id-ext 40)
             Address     0003.E480.75E6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/18           Root FWD 19        128.18   P2p
Fa0/20           Altn BLK 19        128.20   P2p
```